Centre de la sécurité des télécommunications
Communications Security Establishment

NON CLASSIFIÉ

SÉRIE PRATICIENS

CONSEILS EN MATIÈRE DE SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION

GUIDE SUR L'AUTHENTIFICATION DES UTILISATEURS DANS LES SYSTÈMES DE TECHNOLOGIE DE L'INFORMATION

ITSP.30.031 V3

Avril 2018

© Gouvernement du Canada
Le présent document est la propriété exclusive du gouvernement du Canada. Toute modification, diffusion à un public autre que celui visé, production, reproduction ou publication, en tout ou en partie, est strictement interdite sans l'autorisation expresse du CST.

Canada

AVANT-PROPOS

La présente est un document NON CLASSIFIÉ publié avec l'autorisation du chef du Centre de la sécurité des télécommunications (CST). Les propositions de modification devraient être envoyées aux représentants des Services à la clientèle de la Sécurité des TI du CST par l'intermédiaire des coordonnateurs de la sécurité des TI du ministère.

Il est possible de télécharger le présent document à partir du site Web du CST à l'adresse suivante : https://www.cse-cst.gc.ca/fr/publication/list. Pour obtenir de plus amples renseignements, prière de communiquer avec les Services à la clientèle de la Sécurité des TI du CST en envoyant un courriel à itsclientservices@cse-cst.gc.ca ou en appelant le 613-991-7654.

DATE D'ENTRÉE EN VIGUEUR

Le présent document entre en vigueur le (04/04/2018).

[Original signé par]
Scott Jones
Chef adjoint, Sécurité des TI

Le 4 avril 2018
Date

VUE D'ENSEMBLE

Les ministères du gouvernement du Canada (GC) ont recours à des systèmes de technologie de l'information (TI) pour réaliser leurs objectifs opérationnels. Ces systèmes interconnectés sont fréquemment l'objet de menaces susceptibles de perturber sérieusement les opérations du ministère. La compromission des réseaux du GC entraîne des coûts importants et constitue une menace à la disponibilité, à la confidentialité et à l'intégrité des fonds d'information du GC. Certes, les auteurs de menaces sont continuellement à l'affût de nouvelles méthodes d'exploitation des réseaux du GC, mais des mesures d'atténuation peuvent être prises pour protéger efficacement l'infrastructure du GC contre ces modes d'exploitation.

Le document *Conseils en matière de sécurité des technologies de l'information pour les praticiens* (ITSP.30.031 V3) remplace le *Guide sur l'authentification des utilisateurs dans les systèmes de TI* (ITSP.30.031 V2). L'ITSP.30.031 V3 fait également partie d'une série de documents préparés par le CST dans le but de promouvoir la sécurisation des réseaux des ministères du GC. L'authentification des utilisateurs est un impératif de la protection des systèmes ministériels contre les auteurs de cybermenaces, et les contrôles de sécurité employés pour préserver les systèmes du GC représentent, pour leur part, des éléments essentiels de l'élaboration de l'infrastructure de TI.

L'ITSP.30.031 V3 a été préparé dans le but d'aider les praticiens à choisir judicieusement les contrôles de sécurité s'appliquant à l'authentification des utilisateurs. De plus, le document constitue un complément à la *Ligne directrice sur la définition des exigences en matière d'authentification*, du Secrétariat du Conseil du Trésor (SCT) [6].

TABLE DES MATIÈRES

1 Introduction 6

1.1 Facteurs politiques 6

1.2 Environnements concernés 7

1.3 Relation avec le processus de gestion des risques liés à la TI 7

2 Conception d'un mécanisme d'authentification des utilisateurs 9

2.1 Authentification : niveau d'assurance et de robustesse 9

2.2 Exigences visant les mécanismes d'authentification 10

3 Exigences visant la confirmation de l'identité, l'enregistrement et le processus d'émission 11

4 Exigences visant les jetons 12

4.1 Types de jetons 12

4.2 Jetons : menaces et mesures d'atténuation 13

4.3 Jetons : exigences en fonction des LoA 15

5 JETONS : EXIGENCES EN MATIÈRE DE GESTION DES JUSTIFICATIFS 18

5.1 Gestion des jetons et des justificatifs 18

5.2 Gestion des jetons et des justificatifs : menaces et mesures d'atténuation 18

5.3 Gestion des jetons et des justificatifs selon les niveaux d'assurance 19

6 Exigences s'appliquant aux processus d'authentification 20

6.1 Processus d'authentification 20

6.2 Processus d'authentification : menaces et mesures d'atténuation 20

6.3 Processus d'authentification : exigences selon les niveaux d'assurance 21

7 Assertion d'authentification: les exigences 23

7.1 Types d'assertions d'authentification 23

7.2 Assertions d'authentification : menaces et mesures d'atténuation 23

7.3 Assertions d'authentification : exigences selon les niveaux d'assurance 24

8 Exigences en matière de journalisation des événements 27

8.1 Exigences en matière de journalisation pour chaque niveau d'assurance 27

9 Exigences relatives à l'assurance de la sécurité 29

9.1 Assurance de sécurité pour chaque niveau d'assurance 29

10 RÉSUMÉ 30

10.1 Aide et renseignements 30

11 Contenu complémentaire 31

11.1 Liste d'abréviations, d'acronymes et de sigles 31
11.2 Glossaire 32
11.3 Références 38

LISTE DES FIGURES

Figure 1 Processus de gestion des risques à la sécurité des TI 7
Figure 2 Mots de passes conformes, mais faciles à deviner 63

LISTE DES TABLEAUX

Tableau 1 Facteurs d'authentification 12
Tableau 2 Jetons d'authentification 13
Tableau 3 Menaces pesant sur l'authentification 14
Tableau 4 Cadre de niveau d'assurance 40
Tableau 5 Jetons : menaces et mesures d'atténuation 41
Tableau 6 Jetons et vérificateurs : exigences en fonction des niveaux d'assurance (LoA) 44
Tableau 7 Cadre de niveau d'assurance 47
Tableau 8 Gestion des jetons et des justificatifs : menaces et mesures d'atténuation 48
Tableau 9 Gestion des jetons et des justificatifs : exigences en fonction des niveaux d'assurance 50
Tableau 10 Processus d'authentification : menaces et mesures d'atténuation 53
Tableau 11 Assertions d'authentification : menaces et mesures d'atténuation 58

LISTE DES ANNEXES

Annexe A Tables 40
Annexe B Conseils sur la sécurisation des mots de passe 61
B.1 Conseils aux concepteurs de systèmes 61
B.2 Conseils aux opérateurs de systèmes 62
B.3 Conseils aux utilisateurs 63
B.4 Conseils sur l'utilisation des phrases de passe 64

1 INTRODUCTION

Le gouvernement du Canada (GC) compte sur ses systèmes d'information pour soutenir adéquatement les fonctions élémentaires et essentielles de ses opérations ainsi que pour prodiguer des programmes et des services à l'ensemble des Canadiens. En outre, les contrôles de sécurité employés pour préserver les systèmes du GC représentent des éléments essentiels de l'élaboration de l'infrastructure de technologie de l'information (TI). Les contrôles de sécurité s'appliquant à l'authentification influent sur les interactions courantes entre les utilisateurs et les systèmes de TI du GC. Tous les utilisateurs autorisés qui accèdent aux systèmes de TI du GC doivent s'authentifier et le processus d'authentification instaure un niveau acceptable de fiabilité et de confiance au moment d'établir l'identité des utilisateurs.

Le document *Conseils en matière de sécurité des technologies de l'information pour les praticiens* (ITSP.30.031 V3) servira de guide aux praticiens de la sécurité qui seront appelés à choisir les contrôles techniques de sécurité devant s'appliquer aux systèmes exigeant que les utilisateurs soient authentifiés avant d'avoir accès à l'information et aux services leur permettant d'exercer leurs fonctions au sein du gouvernement. Les praticiens des TI responsables du développement d'une solution d'authentification répondant aux exigences de leurs systèmes l'utiliseront conjointement à la *Ligne directrice sur la définition des exigences en matière d'authentification* du SCT [6].

L'ITSP.30.031 V3 remplace l'ITSP.30.031 V2. La version 3 comprend maintenant l'annexe B, *Conseils sur la sécurisation des mots de passe*, qui prodigue des conseils pratiques aux concepteurs de systènes, aux opérateurs de systèmes et aux utilisateurs concernant la conception, la mise en œuvre et l'utilisation de systèmes d'authentification à mot de passe.

Pour obtenir de plus amples informations sur les modes d'établissement des contrôles de sécurité visant les architectures sécurisées, prière de consulter le document du Centre de la sécurité des télécommunications (CST) intitulé ITSG-33 – *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* [1][1].

1.1 FACTEURS POLITIQUES

La sécurisation des réseaux, des données et des actifs du GC passe inévitablement par l'analyse des cybermenaces et des vulnérabilités dont ils font actuellement l'objet et la lutte à celles-ci. Par conséquent, les ministères du GC doivent veiller à ce que les politiques et procédures en matière de sécurité des TI soient mises en œuvre conformément aux politiques du SCT suivantes :

- *Politique sur la gestion des technologies de l'information* [2];
- *Politique sur la sécurité du gouvernement* [3];
- *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information* [4];
- *Ligne directrice sur la définition des exigences en matière d'authentification* [6].

Les conseils techniques contenus dans l'ITSP.30.031 V3 constituent un complément à la *Ligne directrice sur la définition des exigences en matière d'authentification*, du SCT [6], laquelle a pour objet d'assister les responsables de programmes du GC qui sont appelés à établir le niveau approprié d'assurance s'appliquant à l'authentification.

[1] Les numéros entre les crochets renvoient aux documents de référence. Ceux-ci sont énumérés à la section intitulée *Information complémentaire*.

1.2 ENVIRONNEMENTS CONCERNÉS

La présente contient des conseils en matière de TI pour les environnements NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B. Les systèmes utilisés dans les domaines PROTÉGÉ C ou classifiés pourraient nécessiter des mesures additionnelles qui ne sont pas abordées dans le présent document[2]. Conformément à leurs cadres respectifs de gestion des risques, les ministères sont tenus de définir des objectifs de sécurité qui soient propices à la protection des informations et des services ministériels.

1.3 RELATION AVEC LE PROCESSUS DE GESTION DES RISQUES LIÉS À LA TI

Le document *Gestion des risques liés à la sécurité des TI: Une méthode axée sur le cycle de vie* (ITSG-33) [1] propose un ensemble d'activités pour chacun des deux niveaux organisationnels suivants : le niveau ministériel et le niveau des systèmes d'information. La figure 1 dresse un portrait global des activités du niveau ministériel et du niveau des systèmes d'information.

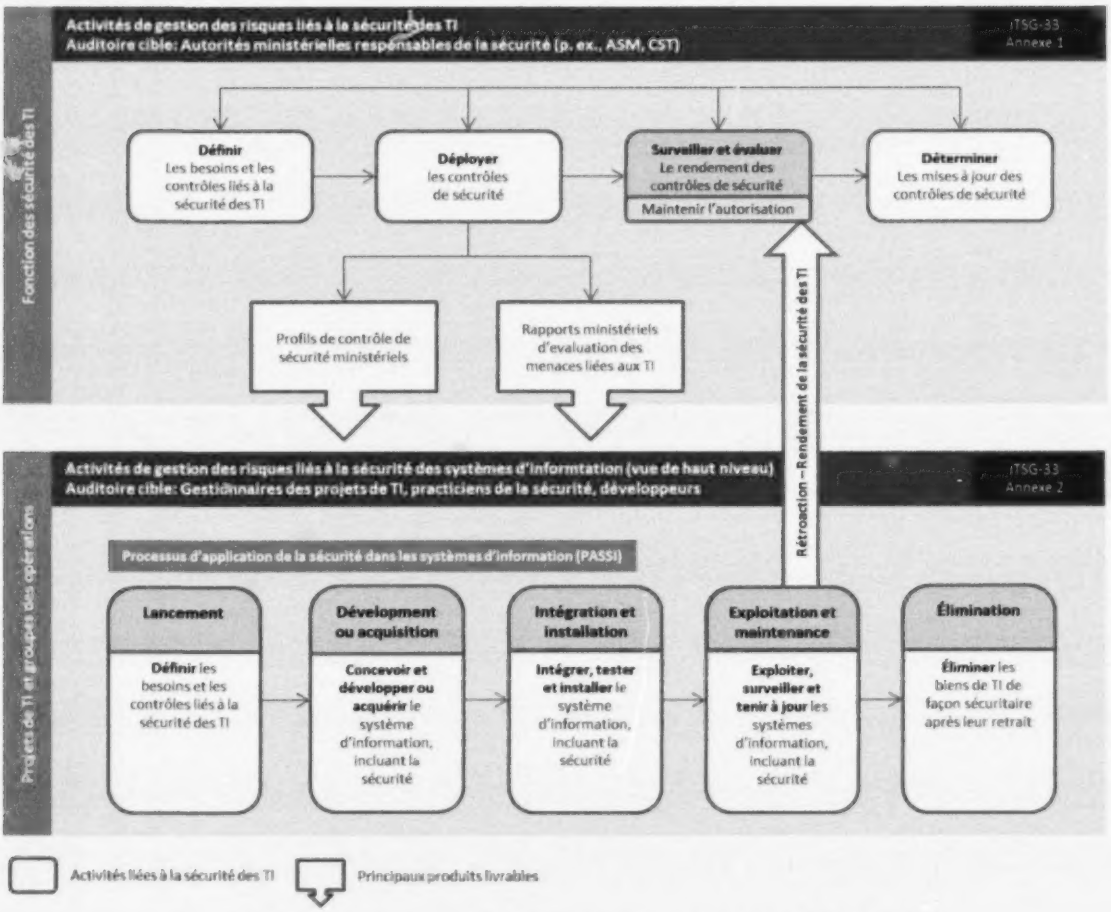

Figure 1 Processus de gestion des risques à la sécurité des TI

[2] Pour obtenir des conseils en matière de TI pour les domaines PROTÉGÉ C ou classifiés, prière de communiquer avec les Services à la clientèle en matière de COMSEC.

Au niveau du ministère, les activités sont intégrées au programme de sécurité de l'organisation pour planifier, gérer, évaluer et améliorer la gestion des risques à la sécurité des TI. En l'occurrence, la teneur de l'ITSP.30.031 V3 devra être prise en compte lors des phases de surveillance et d'évaluation. D'ailleurs, ces activités sont décrites en détail à l'annexe 1 de l'ITSG-33 [1].

Quant aux activités du niveau des systèmes d'information, elles sont intégrées au cycle de vie des systèmes d'information pour s'assurer de répondre aux besoins en matière de sécurité des TI des activités opérationnelles prises en charge et pour veiller à ce que les contrôles de sécurité appropriés soient mis en œuvre et exploités comme prévu, à ce que le rendement des contrôles existants soit évalué en permanence et fasse l'objet de rapports, et à ce que des mesures appropriées soient prises pour corriger toute lacune relevée. En l'occurrence, la teneur de l'ITSP.30.031 V3 devra également être prise en compte lors des phases séquentielles suivantes :

1. lancement;
2. développement ou acquisition;
3. intégration et installation;
4. exploitation et maintenance;
5. élimination.

Ces activités sont décrites en détail à l'annexe 2 de l'ITSG-33 [1].

2 CONCEPTION D'UN MÉCANISME D'AUTHENTIFICATION DES UTILISATEURS

Le présent document contient des conseils techniques sur la sélection judicieuse des contrôles de sécurité en cours d'élaboration de modalités d'authentification des utilisateurs. L'ITSP.30.031 v3 se fonde essentiellement sur deux documents : *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33), du CST [1], et *Electronic Authentication Guideline* (SP 800-63-1) [5], de la National Institute of Standards and Technology (NIST).

L'ITSG-33 [1] présente un processus permettant de choisir les contrôles de sécurité devant s'appliquer aux systèmes et prodigue des conseils visant à adapter ces contrôles de sécurité aux environnements où ils seront mis en œuvre. Pour sa part, le document SP 800-63-2 [5] énonce les exigences ayant particulièrement trait aux systèmes d'authentification.

Nota
La *Ligne directrice sur la définition des exigences en matière d'authentification* du SCT [6] fait mention du présent document. Il s'agit du premier document à consulter avant de définir vos besoins opérationnels et de lancer le processus.

2.1 AUTHENTIFICATION : NIVEAU D'ASSURANCE ET DE ROBUSTESSE

Les conseils prodigués dans l'ITSP.30.031 V3 prennent en compte les quatre niveaux d'assurance (LoA pour *Level of Assurance*) progressifs (du niveau 1 au niveau 4) qui sont définis dans le document SP 800-63-2 [5], du NIST. Le LoA des mécanismes d'authentification convient à diverses catégories de transactions en ligne. Les transactions dont les préjudices (p. ex. ampleur des pertes ou des dommages) résultant de la défaillance d'un contrôle de sécurité d'authentification sont faibles nécessiteront un LoA moins élevé. Dans la même logique, les transactions dont les éventuels préjudices sont importants nécessiteront des niveaux d'assurance plus élevés.

Nota
La *Ligne directrice sur la définition des exigences en matière d'authentification* du SCT [6] emploie la terminologie du *Cadre de niveau d'assurance*, laquelle correspond au *Niveau d'assurance* ou *LoA* adoptée dans la présente. Ces deux terminologies prennent en compte les mêmes niveaux, à savoir les niveaux 1 à 4.

Pour être en mesure d'établir les options d'authentification qui maximiseront les chances de réaliser les LoA visés pour un système donné, les propriétaires opérationnels devraient suivre les conseils énoncés à l'annexe 2 de l'ITSG-33 [1], lesquels prônent une approche permettant de définir le niveau de robustesse (NR) optimal des contrôles en fonction de la catégorie de sécurité des activités opérationnelles et des menaces contre lesquelles il conviendra de protéger l'environnement. Ce NR devrait correspondre aux exigences visant les LoA, conformément à ce qui est énoncé à la section 9 de la présente. Selon les prescriptions formulées à l'annexe 2 de l'ITSG-33, deux éléments caractérisent principalement les niveaux de robustesse :

- **Force de la sécurité** – Caractérisation du potentiel qu'offre un contrôle existant relativement à la protection de la confidentialité, de l'intégrité et de la disponibilité des biens de TI contre les capacités des agents de menace, les risques naturels ou les événements accidentels.

- **Assurance de la sécurité** – Tâches de mise en confiance qui visent à confirmer qu'un contrôle de sécurité a été conçu et mis en œuvre correctement et qu'il fonctionne tel que prévu.

Dans l'ITSP.30.031 V3, on peut trouver une liste des contrôles d'authentification qui répondent aux exigences s'appliquant à la force de la sécurité de chacun des LoA. On y trouve également une définition des catégories d'assurance de la sécurité pour chaque LoA.

Les mécanismes (types de solutions dans les catégories d'exigences en matière de conception de l'authentification) qui, aux fins d'authentification, sont aptes à fournir les forces de sécurité requises pour chaque LoA sont décrits dans les sections 3 à 8. Les exigences qui s'appliquent aux divers LoA sont décrites à la section 9.

L'étape 2 de la *Ligne directrice sur la définition des exigences en matière d'authentification* du SCT [6] concerne les exigences relatives à l'assurance du justificatif et les exigences relatives à l'authentification. De plus, la section 4.4 porte sur les exigences relatives à l'assurance de l'identité. Il importe de noter qu'il n'y a pas nécessairement une adéquation entre le présent document et la *Ligne directrice sur la définition des exigences en matière d'authentification* du SCT [6]. Les deux documents correspondent toutefois sur les points suivants :

- Ligne directrice du SCT, *Exigences relatives à l'assurance de l'identité*, correspond à la section 4 de la présente;
- Ligne directrice du SCT, *Exigences relatives à l'assurance du justificatif*, correspond aux sections 4 et 5 de la présente;
- Ligne directrice du SCT, *Exigences relatives à l'authentification*, correspond aux sections 6, 7, 8 et 9 de la présente.

2.2 EXIGENCES VISANT LES MÉCANISMES D'AUTHENTIFICATION

La sélection d'un mécanisme d'authentification convenant à un niveau de robustesse donné doit tenir compte des exigences s'appliquant à chacune des sept catégories suivantes, lesquelles s'appliquent à la conception des mécanismes d'authentification :

- exigences visant la confirmation de l'identité, l'enregistrement et le processus d'émission;
- exigences visant les jetons;
- exigences visant la gestion des jetons et des justificatifs;
- exigences visant le processus d'authentification;
- exigences visant les assertions;
- journalisation des événements;
- assurance de la sécurité.

Le LoA qui résulte de tout processus d'authentification des utilisateurs est le plus modeste des LoA qui sont associés aux composantes mentionnées précédemment (plus petit commun dénominateur). Les catégories d'exigences en matière de conception de mécanismes d'authentification (voir ci-dessus) sont décrites dans les sections 3 à 9 et énoncent les exigences s'appliquant à chacun des LoA.

3 EXIGENCES VISANT LA CONFIRMATION DE L'IDENTITÉ, L'ENREGISTREMENT ET LE PROCESSUS D'ÉMISSION

Pendant les processus d'enregistrement et d'émission[3], un demandeur se soumet à une épreuve de confirmation de l'identité, laquelle est exécutée par une autorité d'enregistrement (AE) désignée pour vérifier l'identité du demandeur en question. Lorsque cette étape est franchie avec succès, un fournisseur de justificatifs d'identité (FJI) qui entretient un lien de confiance avec l'AE peut enregistrer le demandeur et lui remettre un jeton, puis émettre un justificatif qui lie ce jeton à l'identité du demandeur. Le demandeur peut ensuite utiliser le jeton lorsqu'il agit en tant que requérant au titre du protocole d'authentification qui vise à confirmer l'identité du demandeur auprès d'un système de TI que l'on considère généralement, dans un tel contexte, comme la partie de confiance (PC).

Dans certains systèmes, les requérants interagiront directement avec la PC. Dans d'autres, les requérants doivent confirmer leur identité auprès d'une tierce partie, laquelle fera part de la validité de la demande à la PC, au moyen de ce que l'on appelle une assertion.

La confirmation de l'identité et l'enregistrement du jeton ne sont pas l'objet du présent document. Ces deux facteurs sont traités plus explicitement dans la *Ligne directrice sur la définition des exigences en matière d'authentification* du SCT [6], et les exigences visant leurs LoA sont résumées dans le tableau 1 de l'annexe A.

Pour ce qui concerne le processus global d'authentification, les exigences visant à la fois l'identité et les justificatifs doivent tous être respectées, si l'on tient à réaliser l'intégralité des LoA visés pour un système donné.

[3] Voir la section 4 de la référence [5] pour prendre connaissance du modèle d'authentification et lire les descriptions des parties concernées.

4 EXIGENCES VISANT LES JETONS

Les systèmes d'authentification ont recours à une diversité de facteurs. Les caractéristiques générales de ceux-ci sont décrites au tableau 1.

Tableau 1 Facteurs d'authentification

Caractéristique	Description
Élément connu de l'utilisateur	Information que seul l'utilisateur légitime devrait savoir (p. ex. un mot de passe)
Élément que l'utilisateur possède	Élément matériel que seul l'utilisateur légitime possède et contrôle (p. ex. un jeton matériel)
Élément que l'utilisateur produit ou qui le caractérise	Attribut physique unique à chaque utilisateur (p. ex., empreinte digitale, voix, rétine ou signature)

Plus on ajoute de facteurs d'authentification, plus il est difficile de compromettre les systèmes d'authentification (c'est ce que l'on nomme généralement l'authentification « à deux facteurs » ou « multifactorielle »).

Contrairement aux systèmes d'authentification physique, les systèmes d'authentification électronique ont recours à des facteurs d'authentification qui contiennent un élément secret, dont un requérant se sert pour confirmer auprès d'un « vérificateur » qu'il est bel et bien l'abonné qui est associé au justificatif en question. Dans le présent document, un facteur comportant un tel secret est appelé un « jeton ». Il existe une diversité de jetons d'authentification qui répondent aux différents critères de LoA et de coût, aux exigences de complexité, et aux considérations opérationnelles propres à un système de TI donné.

Pour une utilisation dans un système d'authentification, on a recours à un jeton pour générer des données, lesquelles sont à leur tour soumises à un vérificateur pour confirmer que le requérant possède et contrôle le jeton en question. Les données générées sont également ce que l'on nomme un « authentifiant de jeton ». Certains protocoles permettent le recours à un procédé d'identification (challenge) ou encore à une valeur de défi (ou nonce [nounce]) lorsque l'authentifiant de jeton est généré.

L'authentifiant de jeton se décrit, en quelque sorte, comme l'élément de sortie (output) d'une fonction comportant au moins un élément d'entrée (output) :

authentifiant de jeton = fonction (<secret du jeton> [, <nounce>], [, <challenge>]).

Dans le cas d'un mot de passe, le jeton constitue « en soi » l'authentifiant de jeton.

La présente section décrit brièvement les types de jetons d'authentification faisant l'objet du présent document. Pour chaque type de jeton, la section présente les menaces courantes et les mesures d'atténuation, la gamme des LoA appropriés, et les exigences auxquelles ces jetons doivent répondre pour être utilisés à un LoA donné (dans les limites de la gamme permise).

4.1 TYPES DE JETONS

Les caractéristiques des jetons d'authentification faisant l'objet du présent document sont décrites au tableau 2.

Tableau 2 Jetons d'authentification

Types	Description
Jeton à secret mémorisé	Un secret partagé entre un abonné et un FJI; généralement une suite de caractères ou de chiffres (p. ex. les mots de passe ou les numéros d'identification personnels [NIP])
Jeton à renseignement préenregistré	Série de questions et réponses établie par un utilisateur pendant un processus d'inscription
Élément que l'utilisateur produit ou qui le caractérise	Attribut physique unique à chaque utilisateur (p. ex., empreinte digitale, voix, rétine ou signature)
Jeton secret matriciel[4]	Matrice (électronique ou imprimée) permettant de générer des mots de passe au moyen d'un mécanisme de questions-réponses chaque fois qu'une authentification est nécessaire
Jeton hors bande	Mécanisme combinant un dispositif physique (p. ex. téléphone mobile, téléphone filaire) et un secret transmis au dispositif par un vérificateur chaque fois qu'une authentification est nécessaire
Dispositif de mot de passe à usage unique et à un seul facteur	Dispositif qui génère un mot de passe à usage unique (OTP pour *One-Time Password*), lequel est partagé entre un utilisateur et un vérificateur chaque fois qu'une authentification est requise et qu'il n'est pas nécessaire de recourir à un second facteur d'activation
Dispositif cryptographique multifactoriel	Dispositif qui contient une clé cryptographique protégée et qui ne recourt pas à un second facteur d'activation
Jeton cryptographique multifactoriel (MF)	Clé cryptographique qui est généralement enregistrée dans une clé USB ou dans un autre support de stockage et qui nécessite des facteurs d'activation additionnels. Les facteurs additionnels doivent être ou bien des éléments connus de l'utilisateur ou bien des caractéristiques de l'utilisateur même.
Dispositif de mot de passe multifactoriel à usage unique	Dispositif qui génère un mot de passe à usage unique, lequel est partagé entre un utilisateur et un vérificateur chaque fois qu'une authentification est tentée et qu'il est nécessaire de recourir à un deuxième facteur d'activation. Le deuxième facteur doit être ou bien un élément connu de l'utilisateur ou bien une caractéristique de l'utilisateur même.
Dispositif cryptographique multifactoriel[5]	Dispositif qui contient une clé cryptographique protégée et qui recourt à un deuxième facteur d'activation. Le deuxième facteur doit être ou bien un élément connu de l'utilisateur ou bien une caractéristique de l'utilisateur même.

4.2 JETONS : MENACES ET MESURES D'ATTÉNUATION

Chaque type de jeton d'authentification comporte des vulnérabilités qu'un auteur de cybermenaces pourrait exploiter dans le but d'avoir la mainmise sur un jeton donné.

[4] L'applicabilité d'un jeton secret matriciel imprimé (p. ex. une grille imprimée) consistant en un élément qu'un utilisateur possède (voir la section 4.1) dépend de l'environnement spécifique dans lequel le jeton est utilisé et de la façon dont celui-ci est sécurisé et contrôlé, car le jeton imprimé peut être vulnérable à la duplication non détectée.

[5] Un jeton cryptographique logiciel stocké localement peut être copié s'il n'est pas bien sécurisé. Suivant l'environnement spécifique dans lequel il est utilisé, et la façon dont il est sécurisé et contrôlé, un jeton cryptographique logiciel stocké à distance pourrait ne pas être considéré comme un facteur d'authentification.

Il importe de bien comprendre ces vulnérabilités pour être en mesure de mettre en œuvre des mesures d'atténuation qui conviennent aux LoA envisagés. Par exemple, les jetons matériels peuvent être volés (vulnérabilité), certes, mais en revanche, ils devraient être inviolables (atténuation) de telle sorte que le temps requis pour les reproduire soit plus long que le temps s'écoulant entre le vol et le signalement du vol. De la même façon, les jetons logiciels ou les jetons à concepts préenregistrés (tout comme les jetons matériels qui ne sont pas inviolables) peuvent être reproduits et peuvent servir à ceux qui tentent subrepticement de passer pour le propriétaire d'un jeton donné. Pour cette raison, les systèmes d'authentification associés à des LoA plus élevés ne devraient pas compter uniquement sur les jetons logiciels ou sur les jetons à concepts préenregistrés (ou encore sur les jetons qui ne sont pas dotés de mécanismes d'inviolabilité).

Les menaces qui pèsent sur les facteurs d'authentification entrent dans les catégories décrites au tableau 3.

Tableau 3 Menaces pesant sur l'authentification

Menace	Description
Élément connu de l'utilisateur	Peut être révélé ou encore deviné par un auteur de menaces. L'auteur de menaces pourrait deviner le mot de passe ou le NIP. Un auteur de cybermenace pourrait épier la saisie d'un NIP ou d'un mot de passe, trouver l'inscription d'un NIP ou d'un mot de passe sur une note écrite ou dans un document électronique, ou installer un logiciel malveillant (p. ex. un enregistreur de frappes) conçu pour capter un mot de passe ou un NIP. Dans le cas d'un jeton employé dans le partage d'un secret, un auteur de menaces pourrait se donner accès au FJI ou au vérificateur pour obtenir la valeur dudit secret. De plus, un auteur de menaces pourrait prendre connaissance du secret en captant le trafic de données associé aux demandes confirmées d'authentification et en exécutant des analyses indirectes. Enfin, un auteur de menaces pourrait parvenir à obtenir de l'information sur les renseignements préenregistrés par l'abonné en effectuant des recherches sur celui-ci ou en ayant recours à une diversité de techniques de piratage psychologique.
Élément que l'utilisateur possède	Pourrait être perdu ou encore endommagé, volé ou reproduit par un auteur de menaces. Par exemple, un auteur de menaces qui disposerait d'un accès à l'ordinateur d'un utilisateur pourrait copier un jeton logiciel. Un jeton matériel peut être volé, trafiqué ou reproduit.
Élément que l'utilisateur produit ou qui le caractérise	Peut être reproduit. Un auteur de menaces peut obtenir une copie de l'empreinte digitale du propriétaire d'un jeton et créer une réplique – tout en espérant que le système d'authentification biométrique employé ne soit pas en mesure de bloquer une telle attaque grâce à des techniques robustes de détection du « vivant ».

Voici quelques considérations à prendre en compte lorsqu'il est question d'atténuer les menaces auxquelles s'exposent les jetons d'authentification :

- Les méthodes multifactorielles affaiblissent considérablement les tentatives d'exploits. Ainsi, un auteur de menaces qui envisage de voler un jeton cryptographique et d'en deviner le mot de passe constate que le cumul des facteurs rend la tâche trop difficile. En outre, la combinaison de facteurs qui ne s'exposent pas aux mêmes menaces constitue une approche particulièrement sûre.

- Les mécanismes de sécurité physique peuvent empêcher la reproduction d'un jeton volé. En l'occurrence, les mécanismes de sécurité physique permettent de relever des preuves de trafiquage, de faire de la détection et d'intervenir.
- Les règles relatives à la complexité des mots de passe réduisent les risques qu'un mot de passe soit deviné. Le recours à un mot de passe long qui n'apparaît dans aucun dictionnaire courant peut forcer les auteurs de menaces à tester tous les mots de passe possibles (approche *force brute*).
- Les contrôles de sécurité des systèmes et des réseaux peuvent empêcher les auteurs de menaces d'accéder aux systèmes ou d'installer des logiciels malveillants.
- Les séances de formation périodiques permettent aux abonnés de comprendre quand et comment il faut signaler les compromissions, les soupçons de compromission ou les modèles comportementaux qui pourraient être des signes qu'un auteur de menace tente de compromettre un jeton.
- Les techniques hors-bande permettent de vérifier les preuves de possession de dispositifs enregistrés (p. ex. téléphones cellulaires).

Le tableau 5 de l'annexe A dresse une liste des menaces pesant sur les jetons, propose des exemples pour chaque type de menace et recommande des stratégies d'atténuation visant à contrer ces menaces.

4.3 JETONS : EXIGENCES EN FONCTION DES LOA

Le tableau 6 de l'annexe A dresse une liste des exigences s'appliquant à chaque LoA, et ce, pour les jetons et les vérificateurs employés dans les processus d'authentification.

Ce tableau présente plusieurs des exigences visant à limiter le nombre de tentatives infructueuses d'authentification en verrouillant les comptes utilisateurs dès lors que la limite a été atteinte. Cette approche est une condition essentielle de l'efficacité des systèmes d'authentification, mais il faut savoir qu'elle ouvre la porte aux attaques par déni de service (DoS) (où un auteur de menaces multiplie sciemment les tentatives infructueuses d'authentification). Il conviendra donc de surveiller les systèmes d'authentification pour permettre la détection de tendances inhabituelles d'échec de l'authentification. Il conviendra également de déployer des contrôles de sécurité, notamment les notifications d'ouverture de séances antérieures (avertit l'utilisateur des tentatives d'accès exécutées sur son compte par d'autres utilisateurs) et le temps de verrouillage croissant au fil des tentatives infructueuses. Les contrôles de sécurité suivant, qui sont présentés dans l'annexe 3 de l'ITSG-33 [1], peuvent être intégrés à des solutions conçues sur mesure pour permettre de répondre adéquatement aux exigences :

- AC-7, Tentatives d'ouverture de session infructueuses;
- AC-9, Notification d'ouverture de session précédente (accès);
- AU-2, Événements vérifiables.

Les éléments du tableau qui ont trait aux mots de passe sont assujettis à plusieurs exigences, lesquelles précisent les degrés minimums d'entropie. En l'occurrence, prière de consulter l'annexe A intitulée *Estimating Entropy and Strength*, du document 800-63-2 [5], du NIST, pour obtenir des conseils approfondis sur les méthodes de calcul de l'entropie.

L'établissement de la longueur appropriée d'un mot de passe en se basant sur une estimation de l'entropie constitue une méthode efficace pour les mots de passe aléatoires, mais la qualité de cette estimation se dégrade rapidement lorsque les utilisateurs ont la possibilité de choisir des mots de passe courants ou faciles à deviner. Il conviendra d'ajouter des règles de formation des mots de passe, comme les vérifications dans les dictionnaires et les listes noires de mots de passe, pour empêcher l'usage répété de mots de passe courants.

Il existe également des exigences ayant trait à la durée de vie des mots de passe (politique selon laquelle les mots de passe doivent être changés périodiquement). Les politiques portant sur la durée de vie des mots de passe confèrent les principaux avantages suivants :

- Elles réduisent la période dont disposent ceux qui tentent de craquer ou, dans une moindre mesure, de deviner les mots de passe hors ligne.
- Elles limitent le temps dont les auteurs de menaces disposent pour exploiter un système après la compromission d'un mot de passe.
- Elles rendent plus difficile l'utilisation des mêmes mots de passe dans divers systèmes.

En raison du coût élevé des politiques sur la durée de vie des mots de passe et des inconvénients que ces politiques imposent sur les utilisateurs, on aurait avantage à éviter ce type d'approche, pour peu qu'il soit possible d'obtenir un rendement semblable par l'adoption de contrôles de sécurité additionnels. Par exemple :

- Des techniques adéquates de salage et de hachage ou le chiffrement des fichiers de mots de passe peuvent rendre le craquage des mots de passe quasi impossible pendant la durée de vie d'un système donné.

  L'imposition de règles forçant les utilisateurs à éviter les mots de passe courants que l'on peut facilement deviner de même que l'adoption de mesures adéquates de surveillance des authentifications réduisent les probabilités que les mots de passe soient devinés.

- La surveillance des authentifications permet de mieux détecter les attaques sur les mots de passe et de sensibiliser les utilisateurs à l'existence et à la prévention des compromissions de comptes.

  L'application adéquate de contrôles de sécurité comme l'*avis d'ouverture de sessions antérieures* (AC-9) et l'*examen des événements vérifiables* (AU-2), lesquels sont présentés dans l'ITSG-33 [1], permettent de savoir quand les compromissions ont eu lieu et de réagir efficacement, plutôt que d'attendre de longues périodes avant de pouvoir imposer un changement de mot de passe sur un compte ayant été compromis.

- On peut également recourir à la sensibilisation des utilisateurs pour leur faire comprendre que certaines pratiques, comme le recyclage des mots de passe, posent d'importants risques et pour leur faire adopter de nouvelles pratiques exemplaires.

La gestion de la durée de vie des mots de passe constitue un fardeau pour les utilisateurs et peut inciter ceux-ci à adopter des pratiques inadéquates sur le plan de la sécurité (p. ex. le fait de noter les mots de passe sur des bouts de papier que l'on oublie de placer en lieu sûr). Ainsi, la valeur de ces contrôles sur le plan de la sécurité est discutable. En outre, une durée de vie de 90 jours donne aux auteurs de menaces environ 45 jours pour exploiter les systèmes.

Cette période est amplement suffisante pour un grand nombre d'auteurs de menaces. Une base de données de mots de passe volée qui n'avait été ni hachée, ni salée, ni chiffrée risque fort d'être compromise pendant une telle période. Il est donc recommandé d'éviter l'approche axée sur la durée de vie des mots de passe et de privilégier une approche préconisant la sécurisation des bases de données de mots de passe et la mise en œuvre de mesures de surveillance. Dans ce cas, les changements de mots de passe peuvent être réservés aux occasions où une base de données de mots de passe ou des comptes utilisateurs auraient été censément ou réellement compromis.

4.3.1 JETON : AUGMENTATION DE LOA À LOA3

Lorsque deux jetons – apparaissant au tableau 6 de l'annexe A – sont combinés, il est possible d'élever le LoA de deux jetons LoA2 au niveau d'un seul jeton LoA3 (noter qu'on ne peut pas atteindre un niveau LoA4 par voie de combinaison). Deux éléments sont à considérer lorsqu'on élève un LoA de cette façon :

- Il faut veiller à ce que les deux jetons choisis ne soient pas sensibles aux mêmes vecteurs de menace.
- Pour atténuer le risque de compromission à distance, la paire doit compter un jeton physique qui soit protégé contre les reproductions et les duplications par des mesures de sécurité mises en œuvre dans l'environnement ou par la nature même du jeton en question.

Par exemple, lorsqu'un utilisateur ouvre une session sur un système doté d'un jeton à renseignement secret mémorisé et qu'il utilise un jeton cryptographique logiciel multifactoriel que l'on peut déverrouiller avec un mot de passe provenant de l'ordinateur où le jeton se trouve, tous les éléments peuvent être ainsi volés par le simple recours à un enregistreur de frappes, ce qui ne justifierait pas l'attribution d'un LoA élevé.

Le tableau 7 de l'annexe A présente les LoA qui sont associés aux jetons d'authentification énumérés dans la présente, ainsi que les cas où ils peuvent être combinés de façon à produire l'équivalent d'un jeton LoA3.

Nota
En raison de leur sensibilité aux enregistreurs de frappes et aux maliciels, les jetons cryptographiques logiciels et multifactoriels ne sont pas considérés par la présente – contrairement au document 800-63-2 [5], du NIST – comme répondant, en soi, aux exigences du niveau LoA3.

5 JETONS : EXIGENCES EN MATIÈRE DE GESTION DES JUSTIFICATIFS

Pour maintenir le LoA d'un processus d'authentification, il faut que les justificatifs qui lient les jetons aux identités soient adéquatement gérés tout au long du cycle de vie des jetons et des justificatifs. La présente section porte sur les activités que les FJI doivent entreprendre de façon à maintenir ce lien.

5.1 GESTION DES JETONS ET DES JUSTIFICATIFS

Les FJI sont chargés de générer les justificatifs et de fournir des jetons aux abonnés ou de permettre à ceux-ci d'enregistrer un jeton. Les FJI assument également la gestion de ces jetons et justificatifs.

Les tâches énumérées ci-dessous incombent généralement au FJI :

- **Stockage des justificatifs** – Une fois que les justificatifs ont été créés, un FJI peut se voir confier la responsabilité de les garder en stockage selon le type de jeton (p. ex., un mot de passe doit être conservé dans une base de données de mots de passe).
- **Services de vérification des jetons et des justificatifs** – Dans les cas où le vérificateur et le FJI sont des entités distinctes, celui-ci est responsable de fournir au vérificateur les services de vérification des justificatifs.
- **Renouvellement et réémission des jetons et des justificatifs** – Certains types de jetons et de justificatifs servent aux processus de renouvellement et de réémission. Pendant le renouvellement, l'utilisation ou la période de validité d'un jeton et des justificatifs sont prolongées sans avoir à changer l'identité ou le jeton de l'abonné. Dans le cas d'une réémission, de nouveaux justificatifs sont créés pour l'abonné en même temps qu'une nouvelle identité et qu'un nouveau jeton.
- **Révocation et destruction de jetons et de justificatifs** – Les FJI sont chargés de maintenir l'état de révocation des justificatifs et de détruire ces justificatifs une fois que ceux-ci ont atteint la fin de leur durée de vie. Cette approche peut impliquer des activités comme la création d'une liste de révocation des certificats, laquelle sert à la révocation des certificats publics ou encore à la collecte et à la destruction (mise à zéro) de jetons cryptographiques matériels.
- **Conservation des dossiers** – Le FJI ou son représentant doit consigner les inscriptions et maintenir une chronique des événements et des états (y compris les révocations) pour tous les jetons et les justificatifs qu'il a générés.
- **Contrôles de sécurité** – Les FJI sont chargés de mettre en œuvre et de maintenir les contrôles de sécurité appropriés selon le NR approprié, tel qu'il est indiqué dans l'ITSG-33 [1].

5.2 GESTION DES JETONS ET DES JUSTIFICATIFS : MENACES ET MESURES D'ATTÉNUATION

Les FJI sont chargés de veiller à l'atténuation des menaces pesant sur les activités de gestion des jetons et des justificatifs. Le tableau 5 de l'annexe A fait état des menaces à la confidentialité, à l'intégrité et à la disponibilité des jetons et des justificatifs dont les FJI sont responsables. Il propose également des stratégies d'atténuation qu'il conviendra de mettre en œuvre.

5.3 GESTION DES JETONS ET DES JUSTIFICATIFS SELON LES NIVEAUX D'ASSURANCE

Le tableau 9 de l'annexe A énonce les exigences s'appliquant à la gestion des jetons et des justificatifs en fonction des LoA. Les exigences décrites dans le tableau 9 sont progressives, ce qui signifie que les LoA supérieurs comprennent forcément les exigences des LoA inférieurs.

6 EXIGENCES S'APPLIQUANT AUX PROCESSUS D'AUTHENTIFICATION

Les solutions d'authentification doivent être en mesure d'atténuer un ensemble de menaces au processus d'authentification. La présente section décrit brièvement divers types de processus d'authentification, les menaces qui pèsent sur ces processus et les exigences en matière d'atténuation pour chaque LoA.

6.1 PROCESSUS D'AUTHENTIFICATION

Un protocole d'authentification est une séquence définie de messages circulant entre un requérant et un vérificateur qui sert à démontrer que le requérant dispose d'un jeton valide permettant d'établir son identité. Le protocole peut également montrer au requérant qu'il est en communication avec le vérificateur visé.

Un échange de messages entre un requérant et un vérificateur donnant lieu à une authentification (ou à un échec de l'authentification) entre deux parties est considéré comme le « passage d'authentification ». Pendant ou après un passage d'authentification réussi, une session de communication protégée peut être créée entre les deux parties. Une session protégée peut servir à échanger le reste des messages du passage d'authentification ou à échanger des données de session entre les deux parties.

Des mécanismes de sécurité peuvent être appliqués des deux côtés de la connexion (requérant et vérificateur) pour accroître le niveau de sécurité du processus d'authentification. Par exemple, des ancrages sécurisés peuvent être établis du côté des requérants pour permettre l'authentification des vérificateurs au moyen de mécanismes à clé publique comme le protocole TLS. Semblablement, des mécanismes peuvent être appliqués du côté des vérificateurs pour limiter le nombre des craquages de mots de passe perpétrés par des auteurs de menaces qui tentent d'usurper l'identité de requérants légitimes. En outre, la détection de transactions d'authentification provenant d'un lieu ou d'un canal inattendu de la part d'un requérant ou qui indiquent une configuration fortuite sur le plan matériel ou logiciel peut indiquer un accroissement du niveau de risque et inciter à l'ajout de nouveaux éléments de confirmation de l'identité des requérants.

6.2 PROCESSUS D'AUTHENTIFICATION : MENACES ET MESURES D'ATTÉNUATION

La plupart des menaces décrites dans la présente ont trait à l'exploitation des protocoles d'authentification. Toutefois, les systèmes s'exposent également à des menaces qui n'ont rien à voir avec ces protocoles.

Comme tout autre système, les systèmes d'authentification sont vulnérables aux attaques par déni de service. En plus de s'exposer à d'éventuelles « inondations », les systèmes d'authentification qui utilisent des modalités complexes de chiffrement et de déchiffrement peuvent être submergés par un nombre excessif de demandes d'authentification, et ce, jusqu'à ce que les ressources informatiques visées finissent par flancher. Ce type d'attaque peut être contré en recourant à l'architecture distribuée et aux techniques d'équilibrage des charges.

Les attaques fondées sur le piratage psychologique – lesquelles cherchent à duper les utilisateurs en les incitant à utiliser des protocoles non sécurisés ou à contourner les contrôles de sécurité (p. ex. le fait de tromper un utilisateur en l'incitant à accepter un certificat qui n'est pas validable) – constituent des menaces avec lesquelles il faut composer. Ces menaces peuvent être contrées par la sensibilisation des utilisateurs, la surveillance et la constitution de listes blanches/noires. Cependant, même avec ces mesures d'atténuation en place, il est difficile d'éradiquer la compromission des justificatifs en ayant recours à des mesures de protection contre les attaques issues du piratage psychologique. Pour les systèmes qui sont exploités à des niveaux de LoA supérieurs, il

pourrait être envisageable de renoncer à l'utilisation des clients de courrier électronique ou des navigateurs Web.

Le code malveillant qui s'exécute aux points terminaux (qu'il s'agisse de dispositifs mobiles, d'ordinateurs de bureau ou de portables) représente une autre menace qui doit être prise en compte. Peu importe le niveau de robustesse d'un système d'authentification, la compromission d'un point terminal risque fort de compromettre la sécurité du processus d'authentification. Par exemple, des maliciels peuvent être utilisés pour voler ou exfiltrer des mots de passe et des jetons logiciels (ce qui permet à des auteurs de menaces d'usurper à loisir l'identité d'un utilisateur donné). Les maliciels peuvent également être utilisés pour avoir la mainmise sur un système déverrouillé par un jeton cryptographique matériel, et ce, pendant que le jeton est encore connecté au système. Il conviendra donc de se doter de services de prévention des intrusions d'hôte (HIPS pour *Host-Based Intrusion Protection Services*) et de coupe-feu pour être en mesure d'atténuer les effets de ces menaces.

Le tableau 10 de l'annexe A énumère les menaces à l'authentification de même que les stratégies d'atténuation visant le processus d'authentification.

6.3 PROCESSUS D'AUTHENTIFICATION : EXIGENCES SELON LES NIVEAUX D'ASSURANCE

La présente section présente les exigences correspondant aux LoA, aux fins du processus d'authentification. Les exigences correspondant à chaque LoA sont définies selon les types de menaces à atténuer et le nombre des facteurs qui sont requis.

NIVEAU 1

Le niveau 1 exige que le processus d'authentification soit en mesure d'atténuer l'ensemble des menaces répertoriées, notamment le craquage de mots de passe et la réinsertion (replay).

Tous les jetons à un seul facteur (SF pour *Single Factor*) qui apparaissent dans le tableau 6 de l'annexe A conviennent au niveau 1. Le contrôle des jetons au moyen d'un protocole sécurisé doit être démontré aux fins d'authentification. Les mots de passe ne doivent pas être envoyés en texte clair par voie de réseau. Un simple protocole de sommation-réponse peut être utilisé pour protéger les mots de passe, et il n'est pas obligatoire de chiffrer les données de la session d'authentification. Les secrets partagés à long terme aux fins d'authentification peuvent être révélés au vérificateur.

NIVEAU 2

Le niveau 2 exige que le processus d'authentification soit en mesure d'atténuer les menaces abordées au niveau 1. De plus, un système d'authentification de niveau 2 doit être apte à atténuer les attaques par craquage de mot de passe, par réinsertion, par écoute clandestine et par détournement de session. Il doit également être modérément apte à résister aux attaques de l'intercepteur (MitM pour *Man-in-the-Middle*).

Tous les jetons à un seul facteur (SF pour *Single Factor*) qui apparaissent dans le tableau 6 de l'annexe A conviennent au niveau 2. Le contrôle des jetons au moyen d'un protocole sécurisé doit être démontré aux fins d'authentification. Les données de session échangées entre le requérant et les PC à la suite d'une authentification réussie au niveau 2 seront protégées par un système conçu selon le contrôle SC-8 *Confidentialité et intégrité des transmissions*, qui est décrit dans l'ITSG-33 [1].

NIVEAU 3

Le niveau 3 exige que le processus d'authentification soit en mesure d'atténuer l'ensemble des menaces à l'authentification répertoriées. Un système d'authentification de niveau 3 doit être en mesure d'atténuer les attaques par craquage de mot de passe, par réinsertion, par écoute clandestine, par détournement de session,

par personnification du vérificateur, par hameçonnage et MitM. Le niveau 3 doit à tout le moins offrir une résistance aux attaques MitM.

Le niveau 3 exige une authentification multifactorielle avec au moins deux (2) jetons. Aux fins d'authentification, une preuve de possession des jetons doit être fournie au moyen d'un protocole cryptographique. De plus, au niveau 3, des mécanismes de chiffrement fort devront être utilisés pour protéger le secret des jetons et les authentifiants. S'ils sont utilisés, les secrets partagés à long terme aux fins d'authentification ne seront jamais révélés à quelque partie que ce soit, sauf au requérant et au FJI. Toutefois, les secrets partagés aux fins de sessions (temporaires) peuvent être fournis aux vérificateurs par les FJI, possiblement par l'entremise des requérants. Les techniques cryptographiques approuvées devront être utilisées pour toutes les opérations, y compris le transfert des données de session.

NIVEAU 4

Le niveau 4 exige que le processus d'authentification soit en mesure d'atténuer l'ensemble des menaces à l'authentification répertoriées. Un système d'authentification de niveau 4 doit être en mesure d'atténuer les attaques par craquage de mot de passe, par réinsertion, par écoute clandestine, par détournement de session, par personnification du vérificateur, par hameçonnage, par dévoilement et MitM.

Le niveau 4 exige une authentification à au moins deux facteurs, au moyen d'un dispositif cryptographique multifactoriel ou d'un dispositif multifactoriel à mot de passe à usage unique, que possède un utilisateur.

Le niveau 4 exige une authentification cryptographique forte pour toutes les parties de même que pour tous les transferts de données sensibles entre ces parties. Il conviendra de recourir aux technologies à clé publique ou à clé privée. Conformément à ce qui est énoncé à la section 6.2 de la présente, le secret lié au jeton devra être protégé contre les compromissions résultant de codes malveillants. S'ils sont utilisés, les secrets partagés à long terme aux fins d'authentification ne seront jamais révélés à quelque partie que ce soit, sauf au requérant et au FJI. Toutefois, les secrets partagés aux fins de sessions peuvent être fournis aux vérificateurs ou aux PC par les FJI. Les techniques cryptographiques approuvées par les Federal Information Processing Standards (FIPS) qui sont répertoriées dans le document du CST *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111)* [13] devront être employées pour toutes les opérations, y compris les transferts de données de sessions. Tous les transferts de données sensibles devront être authentifiés par voie cryptographique, au moyen de clés produites par le processus d'authentification, et ce, de façon à opposer une forte résistance aux attaques MitM.

7 ASSERTION D'AUTHENTIFICATION: LES EXIGENCES

Dans les systèmes d'authentification dont les vérificateurs et les PC sont des entités distinctes, les assertions d'authentification servent à transférer, entre des parties connectées à un même réseau, les informations d'identité (et parfois à vérifier les attributs) sur les abonnés. Ces assertions peuvent comporter des énoncés portant sur l'identification et l'authentification des abonnés de même que des énoncés sur les attributs. Parmi les exemples d'assertion, notons les témoins de navigateurs Web, les assertions SAML (Security Assertion Markup Language) et les tickets Kerberos.

Les assertions sont essentielles à la fourniture de services comme la signature unique (SSO pour *Single-Sign-On*) et la fédération des identités. Les assertions fournissent des moyens de partager sécuritairement de l'information sur les abonnés entre les PC, les vérificateurs et les FJI d'un groupe de confiance. L'information contenue dans les énoncés d'attributs d'assertions peut servir à déterminer les privilèges d'accès dans le contrôle d'accès basé sur les attributs (ABAC pour *Attribute-Based Access Control*) et le contrôle d'accès basé sur les rôles (RBAC pour *Role-Based Access Control*).

7.1 TYPES D'ASSERTIONS D'AUTHENTIFICATION

L'authentification fondée sur les assertions se manifeste selon deux modèles : direct et indirect.

Dans le modèle direct, après que l'abonné a été authentifié auprès d'un vérificateur, une assertion est renvoyée à l'abonnée, puis est relayée à une PC.

Dans le modèle indirect, c'est une référence à l'assertion (l'assertion demeurant du côté du vérificateur) qui est relayée à la PC par l'intermédiaire de l'abonné. La PC doit se servir de cette référence pour demander l'assertion auprès du vérificateur, au moyen d'un mécanisme de communication qui n'est pas du ressort de l'abonné.

Les assertions contenant une référence à une clé de chiffrement (c.-à-d. symétrique ou publique) détenue par l'abonnée sont appelées des « assertions de détenteur de clé » (Holder-of-Key Assertions). La clé donne lieu à une méthode permettant à la PC de confirmer que le requérant est bel et bien l'objet de l'assertion. Les assertions qui ne recourent pas à cette méthode sont appelées « assertions du porteur » (Bearer Assertions). Pour atténuer les risques d'usurpation d'identité, des contrôles de sécurité additionnels doivent être employés dans le cas des assertions du porteur.

Prière de consulter le document 800-63-2 [5], du NIST, pour prendre connaissance d'une analyse approfondie des assertions d'authentification.

7.2 ASSERTIONS D'AUTHENTIFICATION : MENACES ET MESURES D'ATTÉNUATION

Dans la présente section, l'on tient pour acquis que les vérificateurs et les PC n'ont pas été compromis. Ainsi, la majorité des menaces viseront un ou plusieurs des éléments suivants :

- la connexion réseau entre un vérificateur, un requérant et une PC;
- la communication du côté du requérant, là où un auteur de menaces peut tenter de modifier les assertions – ou d'en modifier le flux – dans le but d'usurper l'identité d'un abonné ou de rehausser ses propres privilèges.

Le tableau 11 de l'annexe A énumère les menaces qui visent particulièrement les assertions d'authentification et propose des stratégies d'atténuation.

7.3 ASSERTIONS D'AUTHENTIFICATION : EXIGENCES SELON LES NIVEAUX D'ASSURANCE

La présente section fait un résumé des exigences concernant les assertions pour chaque LoA. Toutes les assertions recensées dans la présente ligne directrice indiqueront le LoA de l'authentification initiale d'un requérant auprès d'un vérificateur. L'indication du LoA que comprend l'assertion peut être implicite (p. ex. par l'intermédiaire de l'identité du vérificateur qui indique implicitement le LoA résultant) ou explicite (p. ex. par l'intermédiaire d'un champ explicite compris dans l'assertion).

NIVEAU 1

Au niveau 1, il est essentiel de compliquer la tâche de l'auteur de menaces qui tenterait de falsifier une assertion ou une référence à une assertion pouvant servir à usurper l'identité d'un abonné. Lorsqu'on recourt au modèle direct, l'assertion employée devra être signée par un vérificateur, ou encore, on devra en vérifier l'intégrité grâce à une clé secrète partagée entre le vérificateur et la PC. Lorsqu'on recourt au modèle indirect, la référence à l'assertion qui est employée devra compter au moins 64 bits d'entropie. Quant à l'assertion du porteur, elle ne devra correspondre qu'à une seule transaction. De plus, les références à l'assertion qui sont employées devront être générées sur-le-champ, dès lors qu'une nouvelle assertion est créée par un vérificateur. Autrement dit, les assertions du porteur et les références à l'assertion ne sont générées que pour une seule utilisation.

Dans le but de préserver les assertions contre les modifications pouvant avoir lieu dans un modèle direct, toutes les assertions envoyées depuis le vérificateur vers la PC devront être ou bien signées par le vérificateur ou bien transmises depuis un vérificateur authentifié grâce à une session protégée. Dans un cas comme dans l'autre, un mécanisme fort doit être mis en place et permettre à une PC d'établir une liaison entre la référence à l'assertion et l'assertion en tant que telle, au moyen de communications dont l'intégrité a été protégée ou qui ont été signées par un vérificateur authentifié.

Pour atténuer les répercussions des interceptions d'assertions ou de références à une assertion, il conviendra de faire en sorte que les assertions employées par une PC – une PC qui ne fait pas partie du même domaine Internet que celui du vérificateur – expirent cinq (5) minutes après leur création. Les assertions devant servir dans un seul domaine Internet, y compris les assertions contenues dans les témoins ou faisant référence à ces derniers, peuvent être valides jusqu'à 12 heures.

NIVEAU 2

Il se peut que les justificatifs implicites indiquent que le nom d'abonné répertorié dans une assertion constitue un pseudonyme, ce qui indique une réalité qui doit se refléter dans l'assertion. Les assertions de niveau 2 devront être protégées contre la falsification/la modification, l'interception, le réacheminement et la réutilisation. Les références à l'assertion devront être protégées, quant à elles, contre la falsification, l'interception et la réutilisation. Chaque assertion devra être visée pour une seule PC et, à son tour, la PC devra confirmer qu'il s'agit bien du destinataire visé de l'assertion entrante.

Toutes les stipulations portant sur le niveau 1 s'appliquent. De plus, les assertions, les références à l'assertion et les témoins de session utilisés par un vérificateur ou une PC aux fins d'authentification devront être transmis à un abonné par une session sécurisée qui est liée au processus initial d'authentification de façon à résister efficacement aux attaques par détournement de session (voir le tableau 10 de l'annexe A pour connaître les méthodes pouvant assurer une protection contre ces attaques par détournement de session).

Tant qu'ils seront valides, les assertions, les références à l'assertion et les témoins de session ne seront ni transmis au moyen d'une session non protégée ni envoyés à une entité non authentifiée. Tous les témoins de session employés aux fins d'authentification devront être marqués comme étant sécurisés. Les

réacheminements employés pour envoyer les éléments authentifiants depuis les abonnés jusqu'aux PC indiqueront quel protocole sécurisé (notamment HTTPS) est utilisé.

Pour les protéger contre la falsification, la modification et la divulgation, les assertions qui sont envoyées depuis le vérificateur vers la PC – soit directement soit par l'intermédiaire du dispositif d'un abonné – devront être envoyées au moyen d'une session authentifiée bidirectionnellement et établie entre le vérificateur et la PC, ou seront tout aussi bien signées par le vérificateur et chiffrées pour la PC.

Tous les protocoles d'assertions utilisés à un niveau égal ou supérieur au niveau 2 exigent le recours à des techniques cryptographiques approuvées par FIPS, lesquelles sont énumérées dans le document *ITSP.40.111* [13]. Ainsi, l'emploi des clés Kerberos issues de mots de passe générés par un utilisateur n'est permis ni au niveau 2 ni aux niveaux supérieurs.

NIVEAU 3

Rappelons, en premier lieu, que les exigences relatives au niveau 2 s'appliquent également au niveau 3. De plus, les assertions seront protégées contre la répudiation potentiellement issue des vérificateurs; toutes les assertions employées au niveau 3 devront être signées. Les assertions du niveau 3 devront indiquer les noms vérifiés et non les pseudonymes.

Kerberos a recours à des mécanismes à clé symétrique pour protéger la gestion des clés et les données de session, et n'offre aucune protection contre la répudiation des assertions. Toutefois, compte tenu du degré élevé de confirmation procuré par le protocole Kerberos et de l'étendue de son déploiement, les tickets Kerberos peuvent être utilisés en tant qu'assertions du niveau 3, pour peu que les conditions suivantes soient respectées :

- Tous les vérificateurs (les serveurs d'authentification Kerberos et les serveurs d'attribution des tickets) sont soumis à la gestion d'une seule autorité chargée de veiller à l'exploitation adéquate du protocole Kerberos.
- Tous les abonnés sont authentifiés auprès des vérificateurs au moyen de jetons de niveau 3.
- Toutes les exigences de niveau 3 qui n'ont pas trait à la non-répudiation sont alors respectées.

Au niveau 3, les assertions d'un seul domaine (p. ex. les témoins de navigateurs Web) devront expirer dans les 30 minutes de leur création. Pour leur part, les assertions interdomaines devront expirer dans les cinq (5) minutes de leur création.

Cependant, pour arriver à produire l'effet de la signature unique, les vérificateurs peuvent authentifier les abonnés de nouveau, et ce, avant de produire les assertions à de nouvelles PC, en utilisant une combinaison d'assertions de domaine unique à long et à court terme, pourvu que les conditions suivantes soient respectées :

- L'abonné a été adéquatement authentifié auprès du vérificateur au cours des 12 heures précédentes.
- L'abonné peut montrer qu'il était l'objet de la vérification auprès du vérificateur. Cette confirmation peut se concrétiser, par exemple, par la présence d'un témoin placé par le vérificateur dans le navigateur Web de l'abonné.
- Le vérificateur peut assurément établir si l'abonné a été activement en communication avec la PC depuis la dernière assertion que ce même vérificateur a délivrée. Ce qui signifie que le vérificateur doit obtenir des preuves que l'abonné utilise activement les services de la PC et qu'il n'aurait été inactif que pendant des périodes n'excédant pas 30 minutes. À cet effet, l'assertion d'authentification d'une PC constitue une preuve suffisante.

NIVEAU 4

Au niveau 4, les assertions de porteur (y compris les témoins) ne devront pas être utilisées pour établir l'identité des requérants auprès des PC. Les assertions issues des vérificateurs pourraient toutefois être utilisées pour lier des clés ou d'autres attributs à une identité. Les assertions de détenteur de clé peuvent être utilisées, pourvu que les trois conditions énoncées ci-dessous soient respectées :

- Le requérant est authentifié auprès du vérificateur au moyen d'un jeton de niveau 4 (tel qu'il est établi à la section 4.1) et d'un protocole d'authentification de niveau 4 (conforme aux exigences énoncées à la section 6.3).
- Le vérificateur génère une assertion de détenteur de clé, laquelle fait référence à une clé qui fait partie du jeton de niveau 4 (utilisé pour l'authentification auprès du vérificateur) ou est liée à ce jeton au moyen d'une chaîne de confiance.
- La PC vérifie si l'abonné possède la clé à laquelle il est fait référence dans l'assertion de détenteur de clé, et ce, au moyen d'un protocole de niveau 4.

Les PC devraient tenir un registre des assertions reçues, de façon à ce que les clés examinées par un vérificateur puissent être comparées à la valeur enregistrée auprès d'un FJI. La tenue d'un registre permet à une PC de détecter toute tentative, par un vérificateur, d'usurper l'identité d'un abonné au moyen d'assertions frauduleuses. Cette méthode permet également d'empêcher un abonné de répudier divers aspects du processus d'authentification.

Kerberos emploie des mécanismes à clés symétriques pour protéger la gestion des clés et les données de session, mais ne fournit aucune protection contre la répudiation des assertions, que celles-ci viennent des abonnés ou des vérificateurs. Compte tenu du degré élevé de confirmation procuré par le protocole Kerberos et de l'étendue de son déploiement, les tickets Kerberos peuvent être utilisés en tant qu'assertions du niveau 4, pour peu que les conditions suivantes soient respectées :

- Tous les vérificateurs (les serveurs d'authentification Kerberos et les serveurs d'attribution des tickets) sont soumis à la gestion d'une seule autorité chargée de veiller à l'exploitation adéquate du protocole Kerberos.
- Tous les abonnés sont authentifiés auprès des vérificateurs au moyen de jetons de niveau 4.
- Toutes les exigences de niveau 4 qui n'ont pas trait à la non-répudiation sont alors respectées.
- Les exigences des niveaux 1 à 3 visant la protection des données d'assertion sont intégralement appliquées au niveau 4.

8 EXIGENCES EN MATIÈRE DE JOURNALISATION DES ÉVÉNEMENTS

Il importe non seulement d'authentifier les utilisateurs, mais aussi d'être en mesure de démontrer que l'authentification s'est exécutée avec succès ou qu'elle a échoué pour une raison quelconque. Quoi qu'il en soit, il pourra s'avérer nécessaire de capturer, par quelque moyen, les données transférées entre un utilisateur et un système de TI à des fins probatoires, ces données servant, en quelque sorte, de chaîne de continuité et de preuve de non-répudiabilité. Les ministères et organismes doivent se conformer à toutes les politiques prescrivant la journalisation des événements à des fins d'archivage ou d'accès. En règle générale, il conviendra de suivre les *Lignes directrices concernant la conservation des documents administratifs communs du gouvernement du Canada* [7] pour les documents courants et la section 4 du *Règlement sur la protection des renseignements personnels* [8] pour tous les documents contenant des informations personnelles.

Selon l'emploi des justificatifs d'identité électroniques au sein des services d'un ministère ou d'un organisme et selon le niveau de risque associé aux transactions en ligne, il pourrait être nécessaire de noter la date et l'heure exactes des transactions d'authentification. Pour une sécurisation accrue de l'intégrité, les journaux peuvent être signés numériquement.

Selon la méthode d'authentification utilisée, la traçabilité peut être inhérente (p. ex. dans le cas des signatures numériques) ou peut exiger des interventions manuelles. Pour obtenir des conseils concernant la journalisation, prière de consulter la section sur la famille des contrôles ayant trait à la vérification et à la responsabilisation (VR), dans l'ITSG-33.

8.1 EXIGENCES EN MATIÈRE DE JOURNALISATION POUR CHAQUE NIVEAU D'ASSURANCE

La journalisation des événements d'authentification doit répondre à des exigences indiquant ce qu'il convient d'enregistrer et les modalités de protection des données.

La présente section fait état des exigences concernant la journalisation des événements en fonction des LoA.

NIVEAU 1

Au niveau 1, étant donné la faible valeur ou la nature peu sensible des transactions, il n'est pas nécessaire de journaliser les transactions d'authentification.

NIVEAU 2

Au niveau 2, la journalisation simple des transactions d'authentification est nécessaire. Le mécanisme d'authentification permettra au ministère ou à l'organisme de remonter la procédure d'authentification jusqu'à un utilisateur spécifique et de confirmer les résultats ainsi que l'heure de la procédure. De plus, il conviendra d'instaurer des mécanismes de contrôle permettant de réserver aux seules personnes autorisées l'accès au journal des événements.

NIVEAU 3

Au niveau 3, il est nécessaire de journaliser les transactions d'authentification et de renforcer la sécurité. Le mécanisme d'authentification permettra au ministère ou à l'organisme de remonter la procédure d'authentification jusqu'à un utilisateur spécifique et de confirmer les résultats ainsi que l'heure de la procédure. De plus, le journal des événements doit être protégé au moyen de contrôles d'accès et d'un

mécanisme de détection des tentatives de trafiquage, de manière à détecter les modifications non autorisées apportées aux données du journal des événements (p. ex. à l'aide de signatures numériques).

NIVEAU 4

Au niveau 4, il est nécessaire de journaliser les transactions d'authentification et de renforcer la sécurité. Le mécanisme d'authentification permettra au ministère ou à l'organisme de remonter la procédure d'authentification jusqu'à un utilisateur spécifique et de confirmer les résultats ainsi que l'heure de la procédure. Le journal des événements est protégé au moyen de contrôles permettant de restreindre les accès, d'un mécanisme de détection des tentatives de trafiquage permettant de détecter les modifications non autorisées apportées aux données du journal des événements, et d'un mécanisme de prévention des tentatives de trafiquage (p. ex. support non réinscriptible, système de stockage distribué multiple) grâce auquel on peut prévenir la modification non autorisée des données du journal des événements; ces mesures de protection visent à assurer un degré élevé d'intégrité et de confidentialité des données.

9 EXIGENCES RELATIVES À L'ASSURANCE DE LA SÉCURITÉ

Tel qu'il est indiqué à la section 2.1, l'assurance de sécurité représente le second élément du schéma de robustesse. L'assurance de sécurité de l'authentification constitue, en quelque sorte, l'étalon de mesure de la confiance en la capacité d'un mécanisme d'authentification d'appliquer adéquatement les politiques de sécurité en vigueur (c.-à-d. de remplir ses objectifs de sécurité).

9.1 ASSURANCE DE SÉCURITÉ POUR CHAQUE NIVEAU D'ASSURANCE

Le niveau d'assurance de la sécurité (NAS) qui est présenté à l'annexe 2 de l'ITSG-33 [1] décrit l'ensemble des tâches qu'il convient d'exécuter pendant les étapes de mise en œuvre et d'exploitation afin de garantir la réalisation des objectifs de sécurité. La présente section énonce les exigences s'appliquant à l'assurance de la sécurité en fonction des divers LoA.

NIVEAU 1

Au niveau 1, aucun NAS n'est exigé étant donné la faible valeur ou la nature peu sensible des transactions et l'environnement de menaces mineur.

NIVEAU 2

Au niveau 2, c'est un faible niveau d'assurance de la sécurité qui est exigé, lequel correspond au niveau NAS1 tel qu'il est défini à l'annexe 2 du document *Gestion des risques liés à la sécurité des TI– Une méthode axée sur le cycle de vie* (ITSG-33) [1].

NIVEAU 3

Au niveau 3, c'est un niveau modéré d'assurance de la sécurité qui est exigé, lequel correspond au niveau NAS2 tel qu'il est défini à l'annexe 2 du document *Gestion des risques liés à la sécurité des TI– Une méthode axée sur le cycle de vie* (ITSG-33) [1].

NIVEAU 4

Au niveau 4, on exige le plus élevé des niveaux d'assurance de la sécurité offerts par les produits commerciaux, lequel correspond au niveau NAS3 tel qu'il est défini à l'annexe 2 du document *Gestion des risques liés à la sécurité des TI – Une méthode axée sur le cycle de vie* (ITSG-33) [1]. À ce niveau, les développeurs ou les utilisateurs sont prêts à assumer des coûts additionnels de conception de sécurité.

10 RÉSUMÉ

Les contrôles de sécurité s'appliquant à l'authentification influent sur les interactions courantes entre les utilisateurs et les systèmes de TI du GC. De fait, tous les utilisateurs autorisés à accéder aux systèmes de TI du GC doivent être authentifiés. L'authentification est un processus permettant d'instaurer un niveau acceptable de fiabilité et de confiance au moment d'établir l'identité des utilisateurs.

Le document ITSP.30.031 V3 servira de guide aux praticiens de la sécurité qui seront appelés à choisir les contrôles techniques de sécurité devant s'appliquer aux systèmes qui exigent que les utilisateurs soient authentifiés avant d'avoir accès à l'information et aux services leur permettant d'exercer leurs fonctions au sein du gouvernement. L'ITSP.30.031 V3 décrit également les options offertes à chaque LoA et les exigences qu'il est nécessaire de satisfaire pour atteindre les LoA envisagés.

Pour obtenir de plus amples informations sur les modes d'établissement des contrôles de sécurité visant les architectures sécurisées, prière de consulter le document du CST intitulé *La gestion des risques liés à la sécurité des TI: Une méthode axée sur le cycle de vie* (ITSG-33) [1].

10.1 AIDE ET RENSEIGNEMENTS

Les représentants de votre ministère qui souhaitent obtenir de plus amples renseignements sur l'authentification des utilisateurs pour les systèmes de technologies de l'information peuvent communiquer avec les Services à la clientèle de la STI du CST :

Services à la clientèle de la STI
Téléphone : 613-991-7654
Courriel : itsclientservices@cse-cst.gc.ca

11 CONTENU COMPLÉMENTAIRE

11.1 LISTE D'ABRÉVIATIONS, D'ACRONYMES ET DE SIGLES

Terme	Définition
ABAC	Contrôle d'accès selon les attributs (*AttributeBased Access Control*)
AC	Autorité de certification
AE	Autorité d'enregistrement
CDC	Centre de distribution de clés
CSRF	Falsification de requête intersite (*Cross Site Request Forgery*)
CST	Centre de la sécurité des télécommunications
DoS	Déni de service (*Denial of Service*)
FIPS	Federal Information Processing Standard
FJI	Fournisseur de justificatifs d'identité
GC	Gouvernement du Canada
HIPS	Services de prévention des intrusions d'hôte (*Host-Based Intrusion Protection Services*)
HMAC	Hash Message Authentication Code
ICP	Infrastructure à clé publique
LCR	Liste des certificats révoqués
LoA	Niveau d'assurance (*Level of Assurance*)
MFA	Authentification multifactorielle (*Multi-Factor Authentication*)
MitM	Attaque de l'intercepteur (*Man-in-the-Middle*)
MSM	Module de sécurité matérielle
NAS	Niveau d'assurance de la sécurité
NIP	Numéro d'identification personnel
NIST	National Institute of Standards and Technology
OTP	Mot de passe à usage unique (*One-Time Password*)
PBKDF2	Fonction de dérivation de clés extraction puis expansion 2 (*Password-Based Key Derivation Function 2*)
PC	Partie de confiance
RBAC	Contrôle d'accès selon les rôles (*Role-Based Access Control*)
RL	Niveau de robustesse (*Robustness Level*)
SAML	Langage SAML (*Security Assertion Markup Language*)
SCT	Secrétariat du Conseil du Trésor du Canada
SF	Facteur simple (*Single Factor*)
SP	Publication spéciale (*Special Publication*)

Terme	Définition
SRP	Protocole SRP (*Secure Remote Password*)
SSL	Protocole SSL (*Secure Sockets Layer*)
SSO	Signature unique (*Single Sign-on*)
STI	Sécurité des technologies de l'information
TFA	Authentification à deux facteurs (*Two-Factor Authentication*)
TI	Technologies de l'information
TLS	Sécurité de la couche de transport (*Transport Layer Security*)
URL	Localisateur de ressources uniformes (*Uniform Resource Locator*)
XML	Langage de balisage extensible (*Extensible Markup Language*)
XSS	Faille XSS (*Cross-Site Scripting*)

11.2 GLOSSAIRE

Terme	Définition
Abonné	Partie qui a reçu des justificatifs ou un jeton de la part du FJI.
Approuvé	Approuvé selon FIPS ou recommandé par le CST. Algorithme ou technique qui est spécifié dans la norme FIPS/recommandé par le CST, ou qui est homologué dans la norme FIPS/dans une recommandation du CST.
Assertion	Instruction d'un vérificateur transmise à la PC. Cette instruction contient l'information d'identité concernant un abonné. Les assertions peuvent également contenir des attributs vérifiés.
Assertion de détenteur de clé	Assertion qui contient une référence à des clés symétriques ou à une clé publique (qui correspond à une clé privée) qui sont détenues par un abonné. La PC peut authentifier l'abonné en vérifiant s'il est en mesure de confirmer qu'il est en possession et en contrôle de la clé en question.
Assertion du porteur	Assertion qui ne fournit aucun mécanisme permettant à un abonné de confirmer qu'il en est le détenteur légitime. La PC doit tenir pour acquis que l'abonné qui soumet l'assertion ou la référence à l'assertion en est le détenteur légitime.
Assurance	Dans le contexte de la présente, l'assurance se définit, dans un premier temps, comme étant le degré de confiance dans le processus de vérification employé pour établir l'identité d'un individu à qui des justificatifs ont été émis et, dans un second temps, comme étant le degré de confiance dans le fait que l'individu qui utilise les justificatifs est bel et bien celui à qui ceux-ci ont été émis en premier lieu.
Assurance de base	L'assurance de base correspond aux opérations courantes des réseaux du gouvernement qui sont connectés à Internet. Il s'agit d'une valeur de référence conçue pour assurer la protection des informations sensibles du gouvernement jusqu'au niveau PROTÉGÉ B. Les mesures de sécurité qui sont mises en œuvre dans les pratiques exemplaires et les dispositifs commerciaux, et prescrits dans les conseils sur mesure en matière de sécurité.
Assurance de niveau moyen	Les solutions dont le niveau d'assurance est moyen sont approuvées par le CST aux fins de protection d'informations sensibles du gouvernement, dont le niveau de classification peut aller jusqu'à SECRET. Les mesures de sécurité mises en œuvre se fondent sur un principe favorisant le recours à des produits commerciaux, que l'on répartit sur diverses couches au sein d'une architecture de référence intégrée et approuvée.

Terme	Définition
Assurance élevée	Dans le contexte du GC, les solutions d'assurance élevée reçoivent le soutien d'un programme défini et éprouvé, qui prévoit le recours à des dispositifs cryptographiques et à du matériel de chiffrement fiable. Les mesures de sécurité mises en œuvre servent à protéger les informations les plus sensibles, notamment les opérations ayant trait à la sécurité nationale et au renseignement, lesquelles sont classifiées jusqu'au niveau TRÈS SECRET.
Attaque	Tentative, par une entité non autorisée, de tromper un vérificateur ou une PC en se faisant passer pour un abonné légitime. Tentative, par une entité non autorisée, de tromper un vérificateur ou une PC en se faisant passer pour un abonné légitime ou en fournissant des privilèges non autorisés à son propre compte; ou encore tentative, par quelque entité, d'empêcher les utilisateurs légitimes d'accéder au système d'authentification.
Attaque de l'intercepteur (MitM)	Attaque visant le protocole d'authentification. Un auteur de menace s'interpose entre le requérant et le vérificateur dans le but d'intercepter et de trafiquer les données que le requérant et le vérificateur se transmettent.
Attaque en ligne	Attaque visant le protocole d'authentification, par laquelle un auteur de menace tient le rôle de requérant auprès d'un vérificateur légitime ou trafique le canal d'authentification.
Attaque hors ligne	Attaque par laquelle un auteur de menaces tente d'obtenir des données (p. ex. en se livrant à de l'écoute clandestine sur le passage d'un protocole d'authentification ou en perçant un système pour en subtiliser des fichiers de sécurité) qu'il pourra ensuite analyser dans un système dont il dispose.
Attaque par réinsertion	Attaque par laquelle un auteur de menaces tente de réinsérer des messages interceptés antérieurement (entre un requérant légitime et un vérificateur) dans le but de se faire passer pour ledit requérant auprès du vérificateur ou vice versa.
Attaque par usurpation de l'identité d'un vérificateur	Scénario où un auteur de menaces se fait passer pour un vérificateur pendant le passage d'un protocole d'authentification, généralement dans le but de capturer de l'information pouvant être ultérieurement utilisée pour usurper l'identité d'un requérant auprès du vérificateur en question.
Auteur de cybermenaces	Entité dont les intentions malveillantes l'incitent à compromettre un système d'information.
Authentifiant de jeton	Valeur de sortie générée par un jeton. La capacité à générer sur demande des authentifiants de jeton valides prouve que le requérant possède et contrôle bel et bien un jeton. Les messages de protocole envoyés à un vérificateur sont tributaires d'un authentifiant de jeton, mais ne contiennent pas forcément ce dernier.
Authentifiant secondaire	Secret temporaire émis par un vérificateur à un abonné authentifié en cours de passage d'un protocole de confirmation. Ce secret est ensuite utilisé par l'abonné pour être authentifié auprès d'une PC. Au nombre des exemples d'authentifiants secondaires, notons, entre autres, les assertions du porteur, les références à l'assertion et les clés de session de Kerberos.
Authentification basée sur la connaissance	Authentification d'un individu fondée sur la connaissance de renseignements associés à l'identité qui lui est attribuée dans une base de données publique. La connaissance d'une telle information est personnelle mais non secrète, puisque celle-ci peut être utilisée dans d'autres contextes – que l'authentification auprès d'un vérificateur –, qui n'exigent pas forcément le niveau global d'assurance requis par le processus d'authentification.
Autorité d'enregistrement	Entité de confiance qui établit et atteste l'identité ou les attributs d'un abonné auprès du FJI. Une AE peut constituer une partie intégrante d'un FJI ou peut tout aussi bien être indépendante du FJI,

Terme	Définition
	mais elle garde néanmoins un lien avec celui-ci.
Autorité de certification	Entité de confiance qui émet et révoque les certificats de clés publiques.
Biométrie	Modalité de reconnaissance des individus fondée sur les caractéristiques comportementales ou biologiques desdits individus. Dans la présente, les technologies biométriques peuvent être employées pour déverrouiller les jetons d'authentification et empêcher la répudiation des inscriptions.
Certificat de clé publique	Document numérique émis et signé numériquement par la clé privée d'une AC, qui lie le nom d'un abonné à une clé publique. Le certificat indique que l'abonné qu'il identifie assume seul le contrôle de la clé privée et qu'il est le seul à y accéder. Voir également le document RFC 5280 [9].
Clé privée	Partie secrète d'une biclé asymétrique, que l'on utilise pour les signatures numériques ou pour le déchiffrement de données.
Clé publique	Partie publique d'une biclé asymétrique, que l'on utilise pour la vérification des signatures ou pour le chiffrement de données.
Clé symétrique	Clé employée pour exécuter les deux opérations cryptographiques, par exemple, chiffrer ou déchiffrer ou encore pour créer ou vérifier un code d'authentification de message.
Clés asymétriques	Deux clés qui se correspondent mutuellement, à savoir une clé publique et une clé privée, lesquelles servent à exécuter des tâches complémentaires, notamment le chiffrement et le déchiffrement ou encore la vérification des signatures.
Clés cryptographiques	Valeur servant au contrôle des opérations de cryptographie, notamment le déchiffrement, le chiffrement, la génération de signatures ou encore la vérification de signatures. Aux fins du présent document, les exigences ayant trait aux clés devront être conformes aux exigences minimales énoncées dans le document *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111)* [13], du CST.
Confirmation de l'identité	Processus par lequel un FJI et une autorité d'enregistrement (AE) collectent et vérifient des renseignements concernant une personne pour être en mesure d'émettre à cette dernière des justificatifs essentiels.
Demandeur	Partie assujettie à un processus d'inscription et de vérification de l'identité.
Détournement de session	Attaque par laquelle un auteur de menaces tente de s'immiscer entre un requérant et un vérificateur après un échange d'authentification réussi entre ces deux parties. Ainsi, l'auteur de menaces parvient à se faire passer pour l'abonné auprès du vérificateur – ou vice versa – et à contrôler l'échange de données de session. Les sessions entre le requérant et la PC peuvent être compromises semblablement.
Dévoiement	Attaque par laquelle un auteur de menaces tente de corrompre un service d'infrastructure, notamment le serveur de noms de domaine (DNS pour *Domain Name Service*), de façon à rediriger un abonné vers un faux vérificateur/une fausse PC, ce qui amène l'abonné à révéler de l'information sensible, à télécharger des logiciels malveillants ou à commettre involontairement des actes frauduleux.
Distant	Échange d'information entre des dispositifs qui sont connectés à un réseau où la protection de l'information ne peut être garantie intégralement par les contrôles de sécurité d'une seule organisation. (Mot employé dans les termes « authentification distante » et « transaction distante ».) Tout échange d'information par Internet est considéré comme un échange distant.
Écoute électronique	Tentative que fait un auteur de menaces pour écouter passivement les échanges en cours de

Terme	Définition
	protocole d'authentification, dans le but de capturer de l'information qui pourra lui servir lorsqu'il tentera ultérieurement de se faire passer pour un requérant.
Entropie	Mesure du degré d'incertitude auquel un auteur de menace est confronté lorsqu'il cherche à déceler la valeur d'un secret. L'entropie se mesure généralement en bits.
Faille XSS	Vulnérabilité qui permet à des auteurs de menaces d'injecter des codes/des scripts malveillants dans un autre site Web. Ces segments de codes ou ces scripts acquièrent les permissions accordées aux scripts générés par le site Web ciblé et peuvent dès lors compromettre la confidentialité et l'intégrité des transferts de données entre le site Web en question et le client. Les sites Web sont vulnérables lorsqu'ils affichent des données fournies par les utilisateurs à partir de demandes ou de formulaires, sans veiller à ce que les données en question ne soient pas exécutables.
Falsification de requête intersite (CSRF)	Une CSRF a lieu lorsqu'un abonné dûment authentifié auprès d'une PC et connecté grâce à une session sécurisée navigue vers le site Web d'un auteur de menaces, et qu'il est amené, à son insu, à appeler une action non désirée du côté de la PC. Par exemple, un abonné qui effectue des transactions depuis le site Web d'une banque vulnérable aux CSRF pourrait accidentellement autoriser le transfert d'une importante somme d'argent simplement en cliquant sur le lien malveillant d'un courriel Web pendant qu'une connexion à son compte de banque est encore active sur son ordinateur.
Fonction de hachage	Fonction qui fait correspondre une chaîne de bits de longueur aléatoire à une chaîne de bits de longueur fixe. Les fonctions de hachage approuvées possèdent les caractéristiques suivantes : 1. Unidirectionnelle – Il est infaisable, sur le plan de l'informatique, de trouver une entrée qui corresponde à une sortie prédéterminée. 2. Anticollision – Il est infaisable, sur le plan de l'informatique, de déceler deux entrées distinctes correspondant à une seule et même entrée.
Fournisseur de justificatifs d'identité (FJI)	Entité de confiance qui émet ou enregistre des jetons d'abonnés et qui émet des justificatifs électroniques aux abonnés. Un FJI peut englober les autorités d'enregistrement (AE) et les vérificateurs qu'il exploite. Un FJI peut être une tierce partie indépendante ou encore, il peut émettre des justificatifs qu'il utilisera lui-même.
Hameçonnage	Attaque par laquelle un auteur de menaces tente d'amener un abonné (généralement par voie de courriel) à interagir avec un faux vérificateur/une fausse PC et à révéler de l'information que l'auteur de menaces peut employer ultérieurement pour se faire passer pour un abonné légitime auprès du vrai vérificateur/de la vraie PC.
Identité	Ensemble d'attributs qui décrivent les particularités d'une personne dans un contexte donné.
Infrastructure à clé publique	Ensemble de politiques, de processus, de plateformes serveur, de logiciels et de postes de travail qui servent à administrer les certificats et les biclés publiques-privées, et qui permettent d'émettre, de maintenir et de révoquer des certificats de clés publiques.
Inscription	Processus au cours duquel un demandeur soumet une requête d'abonnement à un FJI, et une PC valide ensuite l'identité du demandeur au nom du FJI.
Jeton	Élément détenu et contrôlé par un requérant (généralement un module cryptographique ou un mot de passe) qui est employé pour confirmer l'identité du requérant.
Jeton cryptographique	Jeton dont le secret consiste en une clé cryptographique.
Justificatif	Objet ou donnée qui lie légitimement une identité (ou d'autres attributs) à un jeton qui est détenu et contrôlé par un abonné.

Terme	Définition
	On tient souvent pour acquis que les justificatifs sont maintenus par un abonné. Toutefois, dans le présent document, le terme désigne également les documents électroniques qui sont tenus par un FJI et qui servent à maintenir le lien réciproque entre le jeton et l'identité d'un abonné.
Justificatif personnel	Justificatifs qui ne doivent pas être révélés par un FJI, car ils pourraient être utilisés pour compromettre le jeton.
Justificatifs faiblement liés	Justificatifs qui décrivent le lien entre un utilisateur et un jeton selon un mode qui peut être modifié sans invalider les justificatifs.
Justificatifs fortement liés	Justificatifs qui décrivent le lien entre un utilisateur et un jeton selon des modes d'inviolabilité.
Kerberos	Protocole d'authentification couramment employé. Pour être authentifiés au moyen de Kerberos, les utilisateurs partagent un mot de passe avec un centre de distribution de clés (CDC). L'utilisateur qui désire communiquer avec un autre utilisateur est d'abord authentifié auprès du CDC, lequel lui remet un « ticket » lui permettant de s'authentifier auprès de cet autre utilisateur.
Langage de balisage extensible	Langage qui renvoie à une classe d'objets appelée « documents XML » (pour *Extensible MarkupLanguage*) et qui décrit le comportement d'un programme informatique qui les traite.
Liste des certificats révoqués	Liste des certificats de clés publiques révoqués. Cette liste est créée et signée numériquement par l'autorité de certification. Voir le document RFC 5280 [9].
Liste noire des mots de passe	Processus par lequel on interdit aux utilisateurs la possibilité d'utiliser des mots de passe figurant à une liste des mots de passe les plus courants ou les plus faciles à deviner.
Mot de passe	Secret qu'un requérant mémorise et utilise pour confirmer son identité. Les mots de passe se constituent généralement de chaînes de caractères.
Multifactoriel	Caractéristique d'un système d'authentification ou d'un jeton qui fait intervenir plus d'un facteur d'authentification. Les trois types de facteurs d'authentification sont les suivants : 1) un élément que l'utilisateur connaît, 2) un élément que l'utilisateur possède ou 3) un élément qui caractérise la personne de l'utilisateur.
Nom vérifié	Le nom d'un abonné qui a été vérifié par confirmation de l'identité.
Nonce (ou valeur de défi)	Valeur qui est employée dans les protocoles de sécurité, mais qui n'est jamais répétée dans une même clé. Par exemple, les nonces employés comme élément de défi dans les protocoles d'authentification de type défi-réponse ne doivent pas être répétés, et ce, jusqu'à ce que les clés d'authentification aient été modifiées. Sinon, on risque une attaque par réinsertion. L'emploi de nonces en tant qu'éléments de défi se distingue du recours au défi aléatoire, en ce qu'un nonce n'est pas forcément imprévisible.
Numéro d'identification personnel	Mot de passe constitué exclusivement de chiffres.
Partie de confiance	Entité qui se fie au jeton et aux justificatifs d'un abonné ou encore à l'assertion d'un vérificateur concernant l'identité d'un requérant pour traiter une transaction ou permettre l'accès à de l'information ou à un système.
Passage du protocole d'authentification	Échange de messages entre un requérant et un vérificateur, qui donne lieu à l'authentification (ou à l'échec de l'authentification).
Phrase de passe	Secret mémorisé qui se compose d'une séquence de mots ou d'un texte que le requérant utilise pour authentifier son identité. La phrase de passe et le mot de passe sont utilisés de manière similaire, mais la première est généralement plus longue pour une sécurité accrue.

Terme	Définition
Piratage psychologique	Fait de gagner la confiance d'un individu dans le but de le tromper et de l'amener à révéler des informations sensibles.
Point d'ancrage de confiance	Clés symétriques ou asymétriques réputées fiables en raison du fait qu'elles font partie intégrante du matériel ou du logiciel ou qu'elles sont fournies par des moyens hors bande, et non parce qu'elles sont garanties par une autre entité de confiance (c.-à-d. dans un certificat de clé publique).
Protocole à connaissance nulle du mot de passe	Protocole d'authentification qui fonctionne avec un mot de passe et qui permet à un requérant d'être authentifié auprès d'un vérificateur sans avoir à lui révéler le mot de passe.
Protocole d'authentification	Une séquence définie de messages circulant entre un requérant et un vérificateur qui sert à démontrer que le requérant dispose d'un jeton valide permettant d'établir son identité et, accessoirement, de montrer au requérant qu'il est en train de communiquer avec le vérificateur voulu.
Protocole SSL (Secure Sockets Layer)	Protocole d'authentification et de sécurité couramment employé par les navigateurs Web et les serveurs Web. Le protocole SSL a été remplacé par le plus récent protocole TLS (Transport Layer Security).
Protocole TLS (Transport Layer Security)	Protocole d'authentification et de sécurité couramment employé par les navigateurs Web et les serveurs Web. Le protocole TLS est défini dans les documents RFC 2246 [10], RFC 3546 [11] et RFC 5246 [12].
Référence à l'assertion	Un objet-données qui est créé avec une assertion et qui identifie un vérificateur en plus de comprendre un pointeur menant à l'assertion intégrale détenue par ce vérificateur.
Remettre à zéro	Écraser l'emplacement d'une mémoire par des données constituées intégralement de bits dont la valeur est « zéro », de façon à ce que les données soient détruites et irrécupérables. Cette procédure se démarque des méthodes de suppressions qui ne font que détruire les références aux données dans un système de fichiers plutôt que les données mêmes.
Requérant	Entité dont l'identité doit être vérifiée au moyen d'un protocole d'authentification.
Réseau	Un média de communication ouvert, généralement l'Internet, qui est employé pour acheminer des messages entre le requérant et d'autres parties. À moins d'avis contraire, rien n'est tenu pour acquis pour ce qui concerne la sécurité du support en question. On suppose simplement qu'il est ouvert et qu'il s'expose à des attaques inopinées de nature active (p. ex. usurpation d'identité, attaque de l'intercepteur, détournement de session) ou passive (p. ex. écoute clandestine) sur le trajet des communications entre les parties (c.-à-d. le requérant, le vérificateur, le FJI ou la PC).
Salage	Valeur non secrète qui est employée dans un processus cryptographique, généralement pour veiller à ce que les résultats du traitement d'une instance ne soient pas réutilisés par un auteur de menaces.
Secret d'authentification	Terme générique désignant toute valeur secrète dont un auteur de menaces peut se servir pour usurper l'identité d'un abonné pendant le protocole d'authentification. Les secrets d'authentification sont également divisés en deux types, soit les secrets d'authentification à court terme et à long terme. Les secrets d'authentification à court terme ne pourraient être utiles à un auteur de menaces que pour une courte période. Le cas échéant, les secrets d'authentification à long terme permettraient à un auteur de menaces d'usurper l'identité d'un abonné jusqu'à ce qu'ils soient modifiés manuellement. En outre, le secret d'un jeton constitue un secret d'authentification à long terme. En revanche, l'authentifiant de jeton, s'il est différent du secret du jeton, constitue un secret d'authentification à court terme.

Terme	Définition
Secret de jeton	Valeur secrète contenue dans un jeton, qui est utilisée pour produire des authentifiants de jeton.
Secret partagé	Secret employé en cours d'authentification, qui est connu du requérant et du vérificateur.
Security Assertion Mark-up Language (SAML)	Une spécification de sécurité axée sur XML et élaborée par OASIS (Organization for the Advancement of Structured Information Standards) aux fins d'échange, par voie d'Internet, d'information d'authentification (et d'autorisation) entre des entités de confiance.
Session protégée	Session dont les messages entre les parties sont chiffrés et dont l'intégrité est assurée par l'emploi de secrets partagés que l'on appelle les « clés de session ». Un participant est considéré comme étant « authentifié » lorsqu'il est parvenu à prouver, pendant la session, qu'il est en possession d'un jeton à long terme et des clés de session, pour peu que l'autre partie soit en mesure de vérifier l'identité correspondant au jeton en question. Lorsque les deux parties sont authentifiées, la session protégée est considérée comme ayant été réciproquement authentifiée.
Témoin	Chaîne de caractères qui est placée dans la mémoire d'un navigateur Web et qui est accessible aux sites Web faisant partie du même domaine que celui du serveur qui a placé le témoin dans le navigateur Web. Les témoins ont plusieurs fonctions. Ils peuvent notamment servir d'assertion ou contenir des pointeurs menant à des assertions.
Tentative de perçage de mot de passe	Attaque par laquelle un auteur de menaces tente à répétition d'ouvrir une session en tentant de deviner les valeurs de l'authentifiant de jeton.
Vérificateur	Entité qui confirme l'identité d'un requérant en vérifiant, par le recours à un protocole d'authentification, si ce requérant est en possession et en contrôle du jeton. À cette fin, un vérificateur pourrait devoir valider les justificatifs qui lient le jeton et l'identité, et vérifier l'état de ceux-ci.

11.3 RÉFÉRENCES

Numéro	Document
1	Centre de la sécurité des télécommunications. *ITSG-33 – La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*, décembre 2014.
2	Secrétariat du Conseil du Trésor du Canada. *Politique sur la gestion des technologies de l'information*, 1er juillet 2007.
3	Secrétariat du Conseil du Trésor du Canada. *Politique sur la sécurité du gouvernement*. 1er juillet 2009.
4	Secrétariat du Conseil du Trésor du Canada. *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information*, sans date.
5	National Institute of Standards and Technology. SP 800-63-2. *ElectronicAuthentication Guideline*, août 2013.
6	Secrétariat du Conseil du Trésor du Canada. *Ligne directrice sur la définition des exigences en matière d'authentification*, novembre 2012.
7	Bibliothèque et Archives Canada. *Lignes directrices concernant la conservation des documents administratifs communs du gouvernement du Canada*, avril 2011.
8	Ministère de la Justice. *Règlement sur la protection des renseignements personnels*, juillet 2015.
9	IETF. RFC 5280. *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, mai 2008.

Numéro	Document
10	IETF. RFC 2246. *The TLS Protocol, Version 1.0*, janvier 1999.
11	IETF. RFC 3546. *Transport Layer Security (TLS) Extensions*, juin 2003.
12	IETF. RFC 5246. *The Transport Layer Security (TLS) Protocol Version 1.2*, août 2008.
13	12 Centre de la sécurité des télécommunications. *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111)*, août 2016.

Annexe A Tables

Le tableau 4 présente les exigences en matière de vérification de l'identité et d'enregistrement des jetons pour chacun des LoA définis dans la *Ligne directrice sur la définition des exigences en matière d'authentification* [6] du SCT.

Tableau 4 Cadre de niveau d'assurance

LoA	Assurance de l'identité	Assurance du justificatif
1	Un faible niveau de confiance est requis pour assurer qu'une personne est celle qu'elle prétend être. Une atteinte à l'intégrité risquerait vraisemblablement de causer un préjudice allant de nul à minime.	Un faible niveau de confiance est requis pour assurer qu'une personne a conservé le contrôle sur un justificatif qui lui a été émis et que ce justificatif n'a pas été compromis. Une atteinte à l'intégrité risquerait vraisemblablement de causer un préjudice allant de nul à minime.
2	Un certain niveau de confiance est requis pour assurer qu'une personne est celle qu'elle prétend être. Une atteinte à l'intégrité risquerait vraisemblablement de causer un préjudice allant de minime à modéré.	Un certain niveau de confiance est requis pour assurer qu'une personne a conservé le contrôle sur un justificatif qui lui a été émis et que ce justificatif n'a pas été compromis. Une atteinte à l'intégrité risquerait vraisemblablement de causer un préjudice allant de minime à modéré.
3	Un niveau de confiance élevé est requis pour assurer qu'une personne est celle qu'elle prétend être. Une atteinte à l'intégrité risquerait vraisemblablement de causer un préjudice allant de modéré à sérieux.	Un niveau de confiance élevé est requis pour assurer qu'une personne a conservé le contrôle sur un justificatif qui lui a été émis et que ce justificatif n'a pas été compromis. Une atteinte à l'intégrité risquerait vraisemblablement de causer un préjudice allant de modéré à sérieux.
4	Un niveau de confiance très élevé est requis pour assurer qu'une personne est celle qu'elle prétend être. Une compromission risquerait vraisemblablement de causer un préjudice allant de sérieux à catastrophique.	Un niveau de confiance très élevé est requis pour assurer qu'une personne a conservé le contrôle sur un justificatif qui lui a été émis et que ce justificatif n'a pas été compromis. Une compromission risquerait vraisemblablement de causer un préjudice allant de sérieux à catastrophique.

Le tableau 5 dresse une liste des menaces pesant sur les jetons, propose des exemples pour chaque type de menace et recommande des stratégies d'atténuation visant à contrer ces menaces.

Tableau 5 Jetons : menaces et mesures d'atténuation

Menaces visant les jetons	Description	Exemple	Stratégies d'atténuation
Vol	Un jeton matériel est volé par un auteur de menaces.	Un dispositif cryptographique matériel a été volé. Un dispositif de mot de passe à usage unique a été volé. Un jeton à secret matriciel a été volé. Un téléphone cellulaire a été volé.	Recourir à des jetons multifactoriels qui doivent être activés au moyen d'un NIP ou par biométrie. Recourir à des jetons inviolables qui se mettent automatiquement à zéro dès qu'un certain nombre de tentatives échouées a été atteint. Enregistrer dans une liste noire les jetons qui ont été compromis.
Découverte	Les réponses aux invites du jeton sont faciles à découvrir au moyen de recherches dans diverses sources de données.	La question « À quelle école avez-vous étudié? » est posée au titre du jeton à renseignements préenregistrés, et la réponse est couramment énoncée dans les médias sociaux.	Sensibiliser les utilisateurs au sujet des moyens qui permettent d'empêcher des entités non autorisées d'utiliser les sites de médias ou les réseaux sociaux pour obtenir ou déduire de l'information non publique sur l'organisation (p. ex. de l'information permettant d'identifier un compte du système ou une personne).
Reproduction	Un jeton a été copié au su ou à l'insu de l'abonné concerné.	Révélation d'un bout de papier sur lequel un mot de passe est inscrit. Des mots de passe enregistrés électroniquement dans un fichier ont été copiés. Un jeton logiciel ICP (clé privée) a été copié. Un jeton matriciel a été copié.	Utiliser des jetons qui sont difficiles à reproduire comme les jetons cryptographiques matériels et inviolables. Veiller à ce que les employés disposent d'un espace de stockage sécurisé pour les jetons imprimés et à ce qu'ils aient reçu de la formation sur l'utilisation de cet espace.

Menaces visant les jetons	Description	Exemple	Stratégies d'atténuation
Écoute clandestine	Le secret ou l'authentifiant du jeton est révélé à un auteur de menaces au moment où un abonné utilise le jeton en question.	Des mots de passe sont appris grâce à l'observation des entrées faites à partir d'un clavier. Des mots de passe sont appris grâce à un logiciel d'enregistrement de frappes. Un NIP est capturé depuis un clavier d'identification personnelle. Des mots de passe sont capturés au terme d'une interception de trafic réseau et d'une analyse de celui-ci.	Établir les jetons au moyen d'un canal distinct. Employer des jetons qui génèrent des authentifiants en fonction de la valeur d'entrée des jetons. Employer des jetons dotés d'authentifiants dynamiques, où la connaissance d'un authentifiant n'a aucune incidence sur la production d'un nouvel authentifiant.
Craquage hors ligne	Un secret de jeton est exposé grâce à des méthodes d'analyse employées en dehors du mécanisme d'authentification.	Une clé est extraite à l'issue d'une analyse différentielle de consommation (DPA pour *Differential Power Analysis*) effectuée sur un jeton cryptographique matériel qui a été volé. Un jeton logiciel ICP est l'objet d'une attaque par dictionnaire qui vise à découvrir le mot de passe permettant de déchiffrer la clé privée.	Employer un jeton qui se verrouille après un nombre défini d'échecs de l'activation. Employer un jeton doté d'un secret à haut degré d'entropie.

Menaces visant les jetons	Description	Exemple	Stratégies d'atténuation
Hameçonnage ou dévoiement	Un secret ou un authentifiant de jeton est capturé par le simple fait de tromper un abonné en faisant passer un auteur de menaces pour un vérificateur ou une PC.	Un abonné révèle un mot de passe à un site Web qui se fait passer pour un vérificateur. Le client d'une banque révèle un mot de passe, lorsqu'il répond à un courriel envoyé par un auteur de menaces qui se fait passer pour une entité représentant légitimement la banque. Un abonné révèle un mot de passe au site Web d'un faux vérificateur après avoir été victime d'un détournement DNS.	Habiliter les employés à distinguer les sites Web légitimes des sites malveillants d'hameçonnage. Sensibiliser les employés au sujet des mesures permettant de réagir adéquatement aux demandes d'ouverture de session ou d'information personnelle, qui sont reçues par courriel, par téléphone ou en mains propres. Mécanismes d'inspection et de filtrage des courriels et des contenus Web, qui ont recours aux services en temps réel de listes noires et de cyberréputation, dans le but d'empêcher que les utilisateurs accèdent à des sites malveillants. Veiller à ce que les serveurs DNS soient en mesure de s'assurer que les réponses aux requêtes DNS viennent de sources réputées. Employer des jetons dotés d'authentifiants dynamiques, où la connaissance d'un authentifiant n'a aucune incidence sur la production d'un nouvel authentifiant.
Piratage psychologique	Un auteur de menaces établit un lien de confiance avec un abonné dans le but de le convaincre de compromettre son jeton ou le secret du jeton.	Un abonné refile son mot de passe à un collègue de bureau qui le lui demande. Un abonné révèle un mot de passe pendant une conversation téléphonique avec un auteur de menaces qui se fait passer pour un administrateur de système.	Sensibiliser les employés au sujet des mesures permettant de réagir adéquatement aux demandes d'ouverture de session ou d'information personnelle, qui sont reçues par courriel, par téléphone ou en mains propres.
Découverte en ligne d'un mot de passe par essai-erreur	Un auteur de menaces se connecte à un vérificateur en ligne et tente de deviner un authentifiant de jeton qui est valide dans le contexte du vérificateur en question.	Des attaques par dictionnaire perpétrées en ligne visent à deviner des mots de passe. Ce type de craquage de mot de passe est employé pour deviner les authentifiants de jetons à mot de passe à usage unique qui sont associés à un requérant légitime.	Appliquer des règles qui empêchent les utilisateurs de se choisir des mots de passe courants et faciles à deviner. Surveiller les tentatives d'authentification et limiter le nombre permis d'échecs d'authentification ainsi que le nombre des tentatives d'authentification. Employer des authentifiants à haut degré d'entropie de façon à rendre les mots de passe indevinables.

Le tableau 6 dresse une liste des exigences s'appliquant à chaque LoA, et ce, pour les jetons et les vérificateurs impliqués dans le processus d'authentification.

Tableau 6 Jetons et vérificateurs : exigences en fonction des niveaux d'assurance (LoA)

Type de jeton	LoA	Exigences visant les jetons	Exigences visant les vérificateurs
Jeton à secret mémorisé	1	Le secret mémorisé peut être ce qui suit : une chaîne de caractères – choisie par l'utilisateur – se composant d'au moins six (6) caractères tirés d'un « alphabet » comptant 90 caractères ou plus; un NIP généré aléatoirement et se composant d'au moins quatre (4) chiffres; un secret doublé d'un degré d'entropie correspondant.	Pour tout compte d'utilisateur, le vérificateur devra mettre en œuvre un mécanisme de ralentissement artificiel du trafic qui parvienne à limiter à 100 le nombre d'échecs d'authentification qu'un auteur de menaces peut essuyer dans une période de 30 jours.
	2	Le secret mémorisé peut être ce qui suit : un NIP généré aléatoirement et se composant d'au moins six (6) chiffres; une chaîne de caractères – générée par l'utilisateur – se composant d'au moins huit (8) caractères tirés d'un « alphabet » comptant 90 caractères ou plus; un secret doublé d'un degré d'entropie correspondant. Le FJI utilise un dictionnaire ou une règle de composition pour imposer des balises aux secrets générés par les utilisateurs. Le FJI met en œuvre une politique prévoyant le recours à des listes noires, ce qui permet d'éliminer d'emblée les secrets que les utilisateurs ont tendance à employer couramment.	Pour tout compte d'utilisateur, le vérificateur devra mettre en œuvre un mécanisme de ralentissement artificiel du trafic qui parvienne à limiter à 100 le nombre d'échecs d'authentification qu'un auteur de menaces peut essuyer dans une période de 30 jours. S'il y a lieu, le vérificateur mettra en œuvre une politique imposant une période de validité des mots de passe n'excédant pas 180 jours.
Jeton à renseignement préenregistré	1	Le secret fournit au moins 14 bits d'entropie. L'entropie correspondant au secret ne peut pas être directement calculée (c.-à-d. questions liées aux renseignements personnels ou générées par une personne). S'il ne fournit pas les questions, l'utilisateur devra sélectionner des invites depuis une liste d'au moins cinq (5) questions.	Pour tout compte d'utilisateur, le vérificateur devra mettre en œuvre un mécanisme de ralentissement artificiel du trafic qui parvienne à limiter à 100 le nombre d'échecs d'authentification qu'un auteur de menaces peut essuyer dans une période de 30 jours. Dans ce cas, une réponse vide n'est pas admissible. Pour tout compte d'utilisateur, le vérificateur devra vérifier les réponses fournies à au moins trois (3) questions et mettre en œuvre un mécanisme de ralentissement artificiel du trafic qui parvienne à limiter à 100 le nombre d'échecs d'authentification qu'un auteur de menaces peut

Type de jeton	LoA	Exigences visant les jetons	Exigences visant les vérificateurs
			essuyer dans une période de 30 jours.
	2	Le secret fournit au moins 20 bits d'entropie. L'entropie correspondant au secret ne peut pas être directement calculée (c.-à-d. questions liées aux renseignements personnels ou générées par une personne). S'il ne fournit pas les questions, l'utilisateur devra sélectionner des invites depuis une liste d'au moins sept (7) questions.	Pour tout compte d'utilisateur, le vérificateur devra mettre en œuvre un mécanisme de ralentissement artificiel du trafic qui parvienne à limiter à 100 le nombre d'échecs d'authentification qu'un auteur de menaces peut essuyer dans une période de 30 jours. Dans ce cas, une réponse vide n'est pas admissible. Pour tout compte d'utilisateur, le vérificateur devra vérifier les réponses fournies à au moins cinq (5) questions et mettra en œuvre un mécanisme de ralentissement artificiel du trafic qui parvienne à limiter à 100 le nombre d'échecs d'authentification qu'un auteur de menaces peut essuyer dans une période de 30 jours.
Jeton secret matriciel	2	L'authentifiant de jeton est doté d'une entropie à 64 bits.	s.o.
		L'authentifiant de jeton est doté d'une entropie d'au moins 20 bits.	Pour tout compte d'utilisateur, le vérificateur devra mettre en œuvre un mécanisme de ralentissement artificiel du trafic qui parvienne à limiter à 100 le nombre d'échecs d'authentification qu'un auteur de menaces peut essuyer dans une période de 30 jours.
Jeton hors bande	2	Le jeton est indépendamment adressable et prend en charge les communications sur un canal distinct du canal principal, aux fins d'authentification.	Le secret généré par le vérificateur devra être doté d'une entropie d'au moins 64 bits. - OU - Pour tout compte d'utilisateur, le secret généré par le vérificateur devra disposer d'au moins 20 bits d'entropie, et le vérificateur devra mettre en œuvre un mécanisme de ralentissement artificiel du trafic qui parvienne à limiter à 100 le nombre d'échecs d'authentification qu'un auteur de menaces peut essuyer dans une période de 30 jours.
Dispositif de mot de passe à usage unique et à un seul facteur	2	Devra utiliser un bloc chiffré ou une fonction de hachage approuvés, tel qu'il est indiqué dans le document du CST, *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111)* [13], de façon à combiner une clé symétrique stockée dans un dispositif à nonce dans le but de créer un mot de passe à usage unique. Le nonce peut être un compteur généré sur le dispositif, ou encore une date et une heure.	Pour les dispositifs synchronisés à mot de passe à usage unique, le mot de passe en question devra avoir une durée de vie qui n'excédera pas 10 minutes. Le module cryptographique qui fait office de vérificateur devra être validé au niveau 1 FIPS 140-2 ou à un niveau supérieur.
Dispositif	2	Le module cryptographique devra être validé au niveau 1	La sortie du jeton générée par le vérificateur (p. ex. un nonce ou un défi)

Type de jeton	LoA	Exigences visant les jetons	Exigences visant les vérificateurs
cryptographique matériel à facteur simple		FIPS 140-2 ou à un niveau supérieur.	sera dotée d'au moins 64 bits d'entropie.
Jeton cryptographique multifactoriel	2	Le module cryptographique devra être validé au niveau 1 FIPS 140-2 ou à un niveau supérieur. Chaque authentification devrait exiger la saisie du mot de passe ou d'une autre donnée d'activation, et la copie non chiffrée de la clé d'authentification devrait être supprimée après chaque authentification.	La sortie du jeton générée par le vérificateur (p. ex. un nonce ou un défi) sera dotée d'au moins 64 bits d'entropie.
Mot de passe multifactoriel à usage unique	4	Le module cryptographique devra être validé au niveau 2 FIPS 140-2 ou à un niveau supérieur; avec une sécurité physique de niveau 3 FIPS 140-2 ou de niveau supérieur. Le mot de passe à usage unique devra être généré par le recours à un bloc chiffré ou à une fonction de hachage approuvés, de façon à combiner une clé symétrique stockée dans un dispositif à nonce dans le but de créer un mot de passe à usage unique. Le nonce peut être une date et une heure, un compteur généré sur le dispositif. Chaque authentification devra exiger la saisie d'un mot de passe ou d'une autre donnée d'activation au moyen d'un mécanisme intégré de saisie.	Pour les dispositifs synchronisés à mot de passe à usage unique, le mot de passe en question devra être une durée de vie de deux (2) minutes ou moins.
Jeton cryptographique matériel et multifactoriel	4	Le module cryptographique devra être validé au niveau 2 FIPS 140-2 ou à un niveau supérieur; avec une sécurité physique de niveau 3 FIPS 140-2 ou de niveau supérieur. Devra exiger la saisie d'un mot de passe, d'un NIP ou d'une donnée biométrique pour activer la clé d'authentification. Ne devra pas permettre l'exportation des clés d'authentification.	La sortie du jeton générée par le vérificateur (p. ex. un nonce ou un défi) sera dotée d'au moins 64 bits d'entropie.

Nota
Le tableau 7 de l'annexe A décrit la façon de combiner les types de jetons de manière à atteindre un niveau LoA3.

Le tableau 7 indique les LoA qui s'appliquent aux jetons d'authentification qui sont répertoriés dans le présent document. Il montre également comment certains jetons peuvent être combinés pour produire l'équivalent d'un jeton de niveau LoA3. Par exemple : en soi, un jeton à secret mémorisé répond au LoA2, mais il peut répondre au LoA3 lorsqu'il est combiné à un jeton à secret matriciel.

Tableau 7 Cadre de niveau d'assurance

	Jetons LoA2							Jetons LoA4	
	Jeton à secret mémorisé	Jeton à renseignement préenregistré	Jeton secret matriciel	Jeton hors bande	Dispositif OTP SF	Dispositif cryptographique SF	Jeton cryptographique MF	Dispositif OTP MF	Dispositif cryptographique MF
Jeton à secret mémorisé	LoA2	LoA2	**LoA3**	**LoA3**	**LoA3**	**LoA3**	LoA2	LoA4	LoA4
Jeton à renseignement préenregistré		LoA2	**LoA3**	**LoA3**	**LoA3**	**LoA3**	LoA2	LoA4	LoA4
Jeton secret matriciel			LoA2	LoA2	LoA2	LoA2	**LoA3**	LoA4	LoA4
Jeton hors bande				LoA2	LoA2	LoA2	**LoA3**	LoA4	LoA4
Dispositif OTP SF					LoA2	LoA2	**LoA3**	LoA4	LoA4
Dispositif cryptographique SF						LoA2	**LoA3**	LoA4	LoA4
Jeton cryptographique MF							LoA2	LoA4	LoA4
Dispositif OTP MF								LoA4	LoA4
Dispositif cryptographique MF									LoA4

Le tableau 8 fait état des menaces à la confidentialité, à l'intégrité et à la disponibilité des jetons et des justificatifs. Il propose également des stratégies d'atténuation qu'il conviendra de mettre en œuvre pour contrer ces menaces.

Tableau 8 Gestion des jetons et des justificatifs : menaces et mesures d'atténuation

Mesure de gestion des jetons et des justificatifs	Menace/ attaque	Exemple	Stratégies d'atténuation
Stockage des justificatifs	Divulgation	Les noms d'utilisateur et les mots de passe stockés dans un fichier système sont divulgués.	Recours à des mécanismes de contrôle assurant une protection contre les divulgations non autorisées des justificatifs stockés. Protection des noms d'utilisateur/des mots de passe au moyen de fonctions sécurisées de salage et de hachage ou de techniques de chiffrement approuvées, de façon à rendre impossible la récupération des mots de passe pouvant résulter de la fuite d'un fichier de mots de passe.
	Trafiquage	Le fichier qui établit la correspondance entre les noms d'utilisateurs et les mots de passe au sein du FJI est piraté, ce qui entraîne une modification des correspondances et le remplacement des mots de passe légitimes par des mots de passe connus d'un auteur de menace.	Recours à des mécanismes de contrôle assurant une protection contre le trafiquage des justificatifs et des jetons.
Services de vérification des jetons et des justificatifs	Divulgation	Un auteur de menaces parvient à visualiser les demandes et les réponses circulant entre un FJI et un vérificateur.	Recours à un protocole de communication qui offre des fonctions de protection de la confidentialité
	Trafiquage	Un auteur de menaces parvient à se faire passer pour un FJI et fournit des réponses erronées aux demandes de vérification de mots de passe d'un vérificateur.	Veiller à ce que les vérificateurs authentifient les FJI avant d'accepter une réponse de vérification de la part de ces FJI. Recours à un protocole de communication qui offre des fonctions de protection de l'intégrité.
	Non-disponibilité	Le fichier de mots de passe ou le FJI ne sont pas disponibles et ne peuvent donc pas fournir les correspondances entre les mots de passe et les noms d'utilisateur.	Veiller à ce que les FJI disposent d'un plan de contingence perfectionné et éprouvé.
		Les vérificateurs ne peuvent obtenir les certificats de clés publiques des requérants parce que les systèmes annuaires sont en panne (p. ex., aux fins de	

Mesure de gestion des jetons et des justificatifs	Menace/ attaque	Exemple	Stratégies d'atténuation
		maintenance ou à la suite d'une attaque par déni de service).	
Émission ou renouvellement ou réémission des jetons et des justificatifs	Divulgation	Le mot de passe d'un abonné est renouvelé par un FJI puis copié par un auteur de menaces pendant que le mot de passe est envoyé par le FJI vers l'abonné.	Recourir à un protocole de communication qui soit apte à protéger la confidentialité des données de session.
	Trafiquage	Un nouveau mot de passe créé par un abonné est modifié par un auteur de menaces pendant que le mot de passe est acheminé à un FJI pour remplacer un mot de passe expiré.	Recourir à un protocole de communication qui soit apte à authentifier le FJI avant l'enclenchement des mesures de réémission des jetons et à protéger l'intégrité des données transmises.
	Émission non autorisée	Un FJI est victime de compromission à la suite d'un accès logique ou physique non autorisé rendu possible par l'émission de justificatifs frauduleux.	Mettre en place des contrôles d'accès physiques et logiques qui soient aptes à prévenir la compromission du FJI. Prière de consulter l'ITSG-33 [4] pour obtenir plus de détails concernant les contrôles de sécurité.
	Renouvellement ou réémission non autorisés	Un auteur de menaces incite frauduleusement un FJI à réémettre un justificatif pour un abonné légitime. Le nouveau justificatif lie l'identité de l'abonné à un jeton fourni par l'auteur de menaces.	Mettre en œuvre une politique exigeant qu'un abonné prouve qu'il a possession du jeton original avant d'en arriver à engager le processus de réémission. Toute tentative d'engagement du processus de réémission au moyen d'un jeton expiré ou révoqué devrait échouer.
		Un auteur de menaces parvient à tirer avantage d'un faible protocole de renouvellement des justificatifs et à prolonger la période de validité des justificatifs d'un abonné légitime.	
Révocation ou destruction des jetons et des justificatifs	Temporisation de la révocation ou de la destruction de justificatifs	Les LCR qui ne sont pas à jour permettent à des auteurs de menaces d'utiliser des comptes périmés (comptes qui pourtant auraient dû être verrouillés suivant la révocation de leurs justificatifs).	Révoquer ou détruire les justificatifs dès que l'avis de révocation ou de destruction des justificatifs a été signifié.
		Les comptes utilisateur ne sont pas supprimés lorsque des employés quittent une entreprise, ce qui crée le risque que des personnes non autorisées se servent des comptes en question.	
	Utilisation de jetons après leur	Un jeton matériel est utilisé après la révocation ou l'expiration des justificatifs correspondants.	Détruire les jetons après la révocation des justificatifs correspondants.

Mesure de gestion des jetons et des justificatifs	Menace/ attaque	Exemple	Stratégies d'atténuation
	mise hors service		

Le tableau 9 énonce les exigences s'appliquant à la gestion des jetons et des justificatifs en fonction des LoA.

Tableau 9 Gestion des jetons et des justificatifs : exigences en fonction des niveaux d'assurance

LoA	Exigences				
	Stockage des justificatifs	Service de vérification des jetons et des justificatifs	Renouvellement/réémission des jetons et des justificatifs	Révocation et destruction des jetons et des justificatifs	Exigence en matière de conservation des documents
1	Les fichiers de secrets partagés employés par les vérificateurs devront être protégés par des contrôles d'accès dans le but de réserver l'accès aux administrateurs ainsi qu'aux applications et au personnel autorisés. Les fichiers de secrets partagés ne devront pas être enregistrés en texte clair. Le hachage unidirectionnel ou une autre fonction semblable doit être employé avant l'enregistrement des fichiers.	Les secrets à long terme des jetons ne devraient pas être partagés avec d'autres parties, sauf en cas de nécessité.	Aucune exigence	Aucune exigence	Aucune exigence
2	Les fichiers de secrets partagés employés par les vérificateurs devront être protégés par des contrôles d'accès dans le but de réserver l'accès aux administrateurs ainsi qu'aux applications et au personnel autorisés. De tels fichiers de secrets partagés ne devront contenir aucun mot de passe ni aucun secret en texte clair. Ainsi, deux options peuvent être employées pour protéger les secrets partagés : 1. Les mots de passe peuvent être	S'ils sont utilisés, les secrets partagés à long terme aux fins d'authentification ne devront jamais être révélés à quelque partie que ce soit, sauf aux vérificateurs relevant des FJI. Toutefois, les secrets partagés aux fins de sessions (temporaires) peuvent être fournis aux	Les FJI devront mettre en œuvre des politiques adéquates de renouvellement et de réémission des jetons et des justificatifs. La preuve de possession d'un jeton encore valide devra être confirmée par le requérant avant qu'un FJI accorde le renouvellement ou la réémission. Les mots de	Les FJI devront révoquer ou détruire les justificatifs et les jetons dans les 72 heures suivant la réception d'un avis indiquant qu'un justificatif n'est plus valide ou qu'un jeton a été compromis, et ce, pour empêcher l'authentification de requérants qui	L'inscription, l'historique et l'état des jetons et des justificatifs (y compris la révocation) devront être enregistrés et conservés par les FJI ou par leur représentant. La période de conservation des données pour les justificatifs de niveau 2 est de sept (7) ans et six mois suivant l'expiration ou la

LoA	Exigences				
	Stockage des justificatifs	Service de vérification des jetons et des justificatifs	Renouvellement/réémission des jetons et des justificatifs	Révocation et destruction des jetons et des justificatifs	Exigence en matière de conservation des documents
	concaténés à une variable de salage (c.-à-d. variable distribuée dans un groupe de mots de passe stockés dans un même espace) puis hachés au moyen d'un algorithme approuvé, faisant ainsi que les calculs informatiques employés pour exécuter une attaque par dictionnaire ou une attaque exhaustive visant un fichier de mots de passe volé deviennent inutiles à l'occasion d'attaques ultérieures sur d'autres fichiers de mots de passe. Les mots de passe hachés sont ensuite enregistrés dans le fichier de mots de passe. Les variables de salage peuvent consister en une fonction de salage global (la même variable pour tous les mots de passe d'un groupe) et en un nom d'utilisateur (un par mot de passe) ou encore en une technique permettant de garantir l'unicité du salage au sein d'un groupe de mots de passe. 2. Les secrets partagés peuvent être chiffrés et enregistrés au moyen de procédures et d'algorithmes approuvés. Les secrets ne doivent être déchiffrés qu'au moment voulu, soit dès lors que l'authentification l'exige. De plus, toute méthode devant servir à la protection des secrets partagés de niveau 3 ou 4 peut également être employée au niveau 2.	vérificateurs par les FJI à des vérificateurs indépendants. Des mesures de protection cryptographiques sont requises pour tous les messages échangés entre un FJI et un vérificateur, qui contiennent des justificatifs personnels ou qui confirment la validité des justificatifs faiblement liés ou possiblement révoqués. Les justificatifs personnels ne devraient être acheminés par voie de sessions protégées à une partie obligatoirement authentifiée, de façon à garantir la confidentialité et à contrer le trafiquage.	passe ne devront pas être renouvelés. Ils seront plutôt réémis. Au terme de la période de validité d'un jeton ou d'un délai de grâce, ni la réémission ni le renouvellement ne devront être autorisés. À la réémission, les secrets de jetons ne devront ni revenir à une valeur par défaut ni être réutilisés. Toutes les transactions devraient se faire par voie de session protégée, notamment par SSL ou par TSL.	s'aviseraient d'employer les justificatifs ou les jetons en question. Lorsqu'il émet des justificatifs qui expirent automatiquement après 72 heures (p. ex. émission quotidienne de nouveaux certificats valides pour 24 heures) un FJI n'est pas tenu de fournir un mécanisme particulier pour révoquer les justificatifs. Les FJI qui enregistrent des mots de passe devraient veiller à ce que la révocation ou la radiation de ceux-ci s'exécute dans les 72 heures.	révocation (l'échéance la plus tardive prévaut) de ces justificatifs.
3	Les fichiers de secrets partagés employés par les vérificateurs devraient	Les FJI devront fournir un mécanisme sécurisé qui	Le renouvellement et la réémission ne devraient	Les FJI devraient disposer d'une	Aucune exigence additionnelle par rapport

LoA	Exigences				
	Stockage des justificatifs	Service de vérification des jetons et des justificatifs	Renouvellement/réémission des jetons et des justificatifs	Révocation et destruction des jetons et des justificatifs	Exigence en matière de conservation des documents
	être protégés par des contrôles d'accès dans le but de réserver l'accès aux administrateurs ainsi qu'aux applications et au personnel autorisés. Les fichiers contenant des secrets partagés doivent être chiffrés. Voici les exigences minimales concernant le chiffrement : 1. La clé de chiffrement pour le secret partagé est elle-même chiffrée selon une clé conservée dans un module cryptographique matériel FIPS 140-2 de niveau 2 ou supérieur ou encore dans un module cryptographique FIPS 140-2 de niveau 3 ou 4; elle n'est déchiffrée qu'au besoin, lorsqu'elle doit faire partie de mesures d'authentification. 2. Les secrets partagés sont protégés en tant que clés dans un module cryptographique matériel FIPS 140-2 de niveau 2 ou supérieur ou encore dans un module cryptographique FIPS 140-2 de niveau 3 ou 4; ils ne sont jamais exportés en texte clair depuis le module en question.	permettra aux vérificateurs et aux PC de vérifier la validité des justificatifs. Ce type de mécanisme peut recourir à des serveurs de validation en ligne ou à des serveurs FJI qui ont accès aux enregistrements de statut pendant les transactions d'authentification. Au nombre des services de vérification offerts par les FJI, des clés temporaires d'authentification de session peuvent être générées par ces FJI à partir de clés de secrets partagés à long terme, puis distribuées à de tiers vérificateurs. Toutefois, les secrets partagés à long terme ne seront, en soi, jamais partagés avec une tierce partie ni même avec les tiers vérificateurs.	avoir lieu qu'avant l'expiration des justificatifs concernés. Dans les cas de renouvellement ou de réémission des justificatifs, les requérants devraient être authentifiés auprès des FJI au moyen du jeton et des justificatifs existants. Toutes les transactions devraient se faire par voie de session protégée, notamment par SSL ou par TSL.	procédure permettant de révoquer les justificatifs et les jetons dans les 24 heures. Les vérificateurs doivent veiller à ce que les jetons employés soient ou bien fraîchement émis (depuis au plus 24 heures) ou bien encore valides. Les systèmes d'authentification fondés sur les secrets partagés peuvent tout simplement supprimer, dans la base de vérification, les noms d'utilisateurs dont l'accès a été révoqué.	au niveau 2.
4	Aucune exigence additionnelle par rapport au niveau 3.	Aucune exigence additionnelle par rapport au niveau 3.	Les transferts de données sensibles devront être authentifiés par voie cryptographique, au moyen de clés liées au processus d'authentification. Toutes les clés temporaires ou à court terme qui sont	Les FJI doivent disposer d'une procédure permettant de révoquer les justificatifs dans les 24 heures suivant l'authentification. Les vérificateurs ou les PC doivent veiller à ce que	Toutes les stipulations relevant des niveaux 2 et 3 s'appliquent. La période minimale de conservation des données constituant les justificatifs de niveau 4 est de dix (10) ans et six (6) mois suivant

LoA	Exigences				
	Stockage des justificatifs	Service de vérification des jetons et des justificatifs	Renouvellement/réémission des jetons et des justificatifs	Révocation et destruction des jetons et des justificatifs	Exigence en matière de conservation des documents
			produites pendant l'authentification initiale devront expirer, ce qui nécessitera une nouvelle authentification dans les 24 heures de l'authentification initiale.	les justificatifs employés soient ou bien fraîchement émis (depuis au plus 24 heures) ou bien encore valides.	l'expiration ou la révocation de ces justificatifs.

Le tableau 10 énumère les menaces à l'authentification de même que les stratégies d'atténuation visant le processus d'authentification.

Tableau 10 Processus d'authentification : menaces et mesures d'atténuation

Type d'attaque	Description	Exemple	Mesures d'atténuation
Découverte en ligne d'un mot de passe par essai-erreur	Un auteur de menaces tente à répétition d'ouvrir une session en tentant de deviner les valeurs de l'authentifiant de jeton.	Un auteur de menaces accède à une page Web et tente d'ouvrir une session au moyen du nom d'un abonné et de mots de passe couramment employés comme « password » ou « secret ».	Un processus d'authentification résistera aux attaques par tentative de deviner en ligne, dans la mesure où les éventuels auteurs de menaces n'ont pas connaissance du jeton d'authentification et ne parviennent pas à deviner les justificatifs malgré leurs tentatives répétées. L'entropie de l'authentifiant, la nature des messages du protocole d'authentification et d'autres mécanismes de gestion (du côté du vérificateur) renforcent cette propriété. Par exemple, les systèmes d'authentification des mots de passe peuvent rendre la découverte de certains mots de passe impossible en imposant l'obligation d'utiliser des mots de passe à entropie élevée et une limite au nombre de tentatives d'authentification ou en contrôlant les intervalles de temps entre ces tentatives. Dans le même ordre d'idées, un vérificateur peut contrer les attaques sur les mots de passe en ajoutant aux contrôles des mesures de surveillance des adresses IP, lesquelles permettent de détecter les attaques moins sophistiquées provenant d'un nombre restreint d'adresses IP, ainsi que des mesures de calcul des statistiques portant sur les tentatives d'authentification, lesquelles permettent de détecter les attaques distribuées.
Hameçonnage	**Hameçonnage** : Un abonné est	Un abonné reçoit un courriel qui	Un processus d'authentification résiste à l'hameçonnage et au dévoiement

Type d'attaque	Description	Exemple	Mesures d'atténuation
et dévoiement	amené, à son insu, à interagir avec un faux vérificateur et à révéler le secret de son jeton ou encore des données personnelles sensibles ou des valeurs d'authentification pouvant être utilisées pour usurper l'identité d'un abonné auprès d'un vérificateur légitime.	l'incite à aller visiter un site Web frauduleux et à employer son nom d'utilisateur et son mot de passe véritables pour ouvrir une session.	(que l'on nomme également usurpation de l'identité d'un vérificateur) dans la mesure où l'usurpateur n'arrive à connaître ni la valeur du secret du jeton ni un authentifiant de jeton pouvant passer pour l'abonné auprès d'un vérificateur légitime. Généralement, ce type d'assurance peut être garanti par les mêmes mécanismes que ceux qui offrent une forte résistance aux MitM (notamment les TLS authentifiés par les clients ou les protocoles spécialisés qui ne permettent au jeton du requérant que de produire un authentifiant à l'intention de vérificateurs valides et préalablement inscrits à une liste). Toutefois, les secrets à long terme peuvent être protégés contre l'hameçonnage et le dévoiement par le simple recours à un jeton inviolable, pourvu que le secret à long terme ne puisse pas être reconstitué à partir d'un authentifiant de jeton. Pour réduire les probabilités d'attaques par hameçonnage ou par dévoiement, il est recommandé que le requérant authentifie les vérificateurs au moyen de mécanismes de chiffrement avant de leur soumettre l'authentifiant de jeton.
	Dévoiement : Un abonné qui tente d'établir une connexion à un vérificateur légitime, mais qui est redirigé vers le site d'un auteur de menace grâce à la manipulation d'un service de nom de domaines DNS ou d'une table de routage.	Un abonné est redirigé vers un site malveillant à la suite du trafiquage d'un DNS, puis révèle ou utilise son jeton en étant persuadé qu'il interagit avec un vérificateur légitime.	
Écoute clandestine	Un auteur de menaces écoute passivement les échanges en cours de protocole d'authentification, dans le but de capturer de l'information qui pourra lui servir lorsqu'il tentera ultérieurement de se faire passer pour un requérant.	Un auteur de menaces capture la transmission d'un mot de passe (ou du hachage d'un mot de passe) entre le requérant et un vérificateur.	Un processus d'authentification résiste aux attaques par écoute clandestine dans la mesure où un écouteur clandestin qui enregistre les messages passant entre un requérant et un vérificateur ne parvient ni à découvrir le secret du jeton du requérant ni à obtenir l'information qui lui permettrait ultérieurement de se faire passer pour un abonné pendant un processus d'authentification. Les protocoles prémunis contre l'écoute clandestine empêchent les auteurs de menaces de perpétrer des attaques hors ligne au cours desquelles les auteurs pourraient enregistrer des passages de protocole d'authentification et les analyser en profondeur depuis leurs propres systèmes dans le but de découvrir le secret d'un jeton ou d'éventuels authentifiants de jeton. Par exemple, un auteur de menaces qui capture les messages du passage d'un protocole d'authentification à mots de passe pourrait tenter de craquer un mot de passe en tentant d'entrer systématiquement tous les mots de passe d'un volumineux dictionnaire et en les comparant aux données du passage de protocole. Les protocoles de session protégés, notamment TLS, résistent bien à l'écoute clandestine.
Réinsertion	Un auteur de menaces tente de	Un auteur de menaces capture le	Un processus d'authentification résiste aux attaques par réinsertion dans la

Type d'attaque	Description	Exemple	Mesures d'atténuation
	réinsérer des messages interceptés antérieurement (entre un requérant légitime et un vérificateur) dans le but de se faire passer pour le requérant auprès du vérificateur.	mot de passe (ou le hachage d'un mot de passe) d'un requérant à partir d'une session d'authentification, puis le soumet à un vérificateur dans le but de se donner ultérieurement un accès.	mesure où il est pratiquement impossible de réussir une authentification en enregistrant puis en réinsérant le message d'une authentification antérieure. Les protocoles qui font appel aux nonces ou aux défis pour prouver la « **récence** » de la transaction résistent aux attaques par réinsertion, puisqu'un vérificateur sera en mesure d'établir que les vieux messages de protocole ne contiennent ni les nonces appropriés ni les données temporelles relatives à la session d'authentification en cours.
Détournement de session	Un auteur de menaces parvient à s'immiscer entre un abonné et un vérificateur après un échange d'authentification réussi entre ces deux parties. Ainsi, l'auteur de menace parvient à se faire passer pour un abonné auprès d'un vérificateur ou d'une PC – ou vice versa – et à contrôler l'échange de données de session.	Un auteur de menaces parvient à prendre en charge une session déjà authentifiée à la suite d'écoute clandestine ou de la découverte de la valeur d'authentification des fichiers témoins qui servent aux demandes HTTP envoyées par un abonné.	La combinaison d'un processus d'authentification et d'un protocole de transfert de données résiste aux détournements dans la mesure où l'authentification est liée au transfert de données, de façon à empêcher tout adversaire de prendre part activement et furtivement à la session de transfert de données établie entre un abonné et un vérificateur ou une PC. Il s'agit là d'une propriété de la relation entre le protocole d'authentification et le protocole de session subséquent qui sert à transférer les données. Ce lien se concrétise généralement après avoir généré un secret partagé bon pour une session pendant le processus d'authentification, celui-ci permettant ultérieurement à un abonné et à un vérificateur ou une PC d'authentifier le transfert de toutes les données de session. Il importe de noter que les applications Web, même celles qui disposent de protection SSL/TLS, peuvent être vulnérables à un type de détournement de session appelé « falsification de requête intersite » (CSRF pour *Cross Site Request Forgery*). Le processus de CSRF comprend un site malveillant qui contient un lien menant à l'adresse URL d'une PC légitime. Le site malveillant est généralement conçu pour que les navigateurs Web envoient automatiquement une demande HTTP à une PC dès lors qu'ils visitent ce site malveillant. Lorsqu'un abonné visite le site malveillant après avoir ouvert une session SSL/TLS auprès d'une PC, la demande est généralement envoyée dans la même session tout en laissant intacts les fichiers témoins d'authentification. Même si l'auteur de menaces n'obtient jamais l'accès au secret de session, la demande peut être conçue de façon à produire des effets secondaires, notamment l'envoi d'un courriel ou l'autorisation du transfert d'une importante somme d'argent. On peut prévenir les attaques CSRF en veillant à ce que ni un auteur de menaces ni un script s'exécutant sur le site de ce dernier ne disposent d'une information suffisante pour créer une demande valide qui

Type d'attaque	Description	Exemple	Mesures d'atténuation
			autoriserait quelque mesure (dont les conséquences seraient considérables) de la part d'une PC. Il suffit d'insérer des données aléatoires fournies par une PC dans toute adresse URL provoquant des effets secondaires et dans un champ caché faisant partie des formulaires du site Web d'une PC. Ce mécanisme, toutefois, ne procure pas les effets escomptés lorsque l'auteur de menaces est en mesure d'exécuter des scripts sur le site d'une PC (faille XSS). Pour prévenir les vulnérabilités XSS, une PC doit nettoyer les entrées provenant de requérants ou d'abonnés dans le but de s'assurer que ces entrées ne contiennent pas d'exécutable ou, à tout le moins, qu'elles ne sont pas malveillantes, et ce, avant que les entrées s'affichent en tant que contenu dans le navigateur de l'abonné.
Attaque de l'intercepteur	Un auteur de menaces s'interpose entre le requérant et le vérificateur dans le but d'intercepter et de trafiquer le contenu des messages du protocole d'authentification. Un auteur de menaces se fera généralement passer pour un vérificateur auprès d'un requérant tout en se faisant passer pour un requérant auprès d'un vérificateur. Le fait de prendre part à des échanges simultanés avec les deux parties peut permettre à un auteur de menaces de se servir des messages d'authentification envoyés par une partie légitime pour s'authentifier auprès d'une autre.	Un auteur de menaces accède au contenu d'un routeur qui achemine des messages entre un vérificateur et un requérant. Au moment de réacheminer les messages, un auteur de menaces substitue sa propre clé publique à celle du vérificateur. À son insu, le requérant chiffre son mot de passe avec une clé qui permet à l'auteur de menaces de déchiffrer le mot de passe. Un auteur de menaces conçoit un site Web frauduleux qui se fait passer pour un vérificateur légitime. Lorsqu'un requérant non vigilant tente d'ouvrir une session au moyen de son dispositif à mot de passe à usage unique, le site de l'auteur de menaces utilise, dans le même temps, le mot de passe à usage unique du requérant pour ouvrir une session du côté du vérificateur.	Les protocoles d'authentification résistent aux tentatives de MitM dans la mesure où les deux parties (c.-à-d. le requérant et le vérificateur) s'authentifient réciproquement de façon à prévenir la participation furtive d'une tierce partie. Il y a deux niveaux de résistance : **Résistance faible aux MitM** – Un protocole offre une faible résistance aux attaques MitM lorsqu'il dispose d'un mécanisme qui permet au requérant de savoir s'il interagit véritablement avec un vérificateur légitime, mais qui lui fait tout de même courir le risque de révéler l'authentifiant de jeton (à une partie non autorisée), lequel peut ultérieurement permettre d'usurper l'identité du requérant auprès du vérificateur légitime. Par exemple, l'envoi d'un mot de passe par TLS authentifié par un serveur est faiblement résistant aux attaques MitM. Le navigateur permet au requérant de vérifier l'identité du vérificateur. En revanche, si le requérant n'est pas suffisamment vigilant, le mot de passe sera révélé à une partie non autorisée qui pourrait employer l'information abusivement. Une résistance faible aux MitM peut également être fournie par un protocole à connaissance nulle du mot de passe, notamment l'échange chiffré de clés (EKE pour *Encrypted Key Exchange*), l'échange de clés exponentielles à authentification de mot de passe simple (SPEKE pour *Simple Password-authenticated Exponential Key Exchange*) ou le protocole SRP (Secure Remote Password), lesquels permettent à un requérant de s'authentifier auprès d'un vérificateur sans avoir à divulguer le secret de son jeton. Toutefois, un auteur de menaces aurait la possibilité de se jouer du requérant en amenant celui-ci à laisser un protocole à faible sécurité traiter son mot de passe, ce qui aurait pour effet de révéler ce dernier à l'auteur

Type d'attaque	Description	Exemple	Mesures d'atténuation
			de menace en question. De plus, s'il est déraisonnablement difficile, pour le requérant, de s'assurer qu'un protocole adéquat est employé, il faut conclure que le processus d'authentification n'offre pas le minimum requis, soit une résistance faible aux MitM (p. ex. lorsqu'un protocole à connaissance nulle du mot de passe est mis en application par un applet Java non signé et affiché dans une page HTTP en texte clair).

Le tableau 11 énumère les menaces qui visent particulièrement les assertions d'authentification et propose des stratégies d'atténuation.

Tableau 11 Assertions d'authentification : menaces et mesures d'atténuation

Type de menace à l'assertion	Menace particulière	Stratégies d'atténuation
Compromission des données d'assertion Les menaces de ce type ciblent généralement les assertions dans le but d'obtenir ou de modifier les données d'assertion (ou les références à l'assertion) de façon à permettre l'usurpation de l'identité d'un abonné aux fins d'accès non autorisé à des données et des services.	**Fabrication/modification d'assertion** – Un auteur de menaces peut générer une fausse assertion ou modifier le contenu d'une assertion légitime (notamment les énoncés d'authentification ou d'attribut), ce qui amène la PC à accorder des accès inappropriés à un abonné. Par exemple, un auteur de menaces pourrait modifier une assertion de façon à en prolonger la période de validité. Pour sa part, un abonné pourrait modifier une assertion de façon à se donner accès à de l'information qu'il ne serait normalement pas autorisé à visualiser.	Pour se prémunir contre les divulgations d'assertions et contre les fabrications/les modifications d'assertions, il faut principalement recourir à ce que l'on conçoit comme une session protégée par authentification réciproque – ou une mesure équivalente – entre le vérificateur et la PC. Tout protocole nécessitant qu'une série de messages entre deux parties soient signés par leurs destinateurs respectifs et chiffrés à l'intention des destinataires fournit les mêmes garanties que celles qui sont offertes par une session protégée par authentification réciproque et est considéré, par conséquent, comme un équivalent. L'assertion peut être signée numériquement par un vérificateur. Une PC doit vérifier la signature numérique pour s'assurer que celle-ci a été émise par un vérificateur légitime. L'assertion peut être envoyée par voie de session protégée, notamment par TLS. Pour protéger l'intégrité des assertions contre les tentatives malveillantes, les vérificateurs devront être authentifiés.
	Divulgation d'assertion – Les assertions peuvent contenir des énoncés d'authentification ou d'attribut, lesquelles contiennent de l'information sensible sur l'abonné. La divulgation des contenus d'assertions peut vulnérabiliser l'abonné à d'autres types d'attaques.	Pour se prémunir contre les divulgations d'assertions et contre les fabrications/les modifications d'assertions, il faut principalement recourir à ce que l'on conçoit comme une session protégée par authentification réciproque – ou une mesure équivalente – entre le vérificateur et la PC. Tout protocole nécessitant qu'une série de messages entre deux parties soient signés par leurs destinateurs respectifs et chiffrés à l'intention des destinataires fournit les mêmes garanties que celles qui sont offertes par une session protégée par authentification réciproque et est considéré, par conséquent, comme un équivalent. L'assertion peut être envoyée par voie de session protégée à une PC authentifiée. Les assertions signées par un vérificateur peuvent être chiffrées à l'intention d'une PC spécifique sans autre mesure de protection de l'intégrité.
	Répudiation d'une assertion par un vérificateur – Une assertion pourrait être répudiée par un vérificateur lorsque les mécanismes appropriés n'ont pas été mis en œuvre. Par exemple, un vérificateur qui n'appose pas une signature numérique à une assertion peut déclarer que celle-ci n'a pas été générée par ses propres services.	L'assertion peut être signée numériquement par un vérificateur au moyen d'une clé qui prend en charge la non-répudiation. Une PC doit vérifier la signature numérique pour s'assurer que celle-ci a été émise par un vérificateur légitime.

Type de menace à l'assertion	Menace particulière	Stratégies d'atténuation
	Répudiation d'une assertion par un abonné – Un abonné compromis ou malveillant peut émettre des assertions à la mauvaise entité. Par conséquent, un abonné peut répudier une transaction effectuée avec une PC qui a été authentifiée simplement par une assertion du porteur.	Un vérificateur peut émettre des assertions de détenteur de clé plutôt que des assertions de porteur. Dans ce cas, un abonné peut prouver qu'il est en possession de la clé validée (assertion) auprès d'une PC. Si les clés validées coïncident avec le justificatif à long terme de l'abonné (fourni par un FJI), il sera évident pour toutes les parties concernées que c'est bien l'abonné qui a été authentifié auprès de la PC, et qu'il ne s'agit pas d'un vérificateur qui se ferait passer pour l'abonné.
	Redirection d'assertion – Un auteur de menaces se sert de l'assertion générée par une PC dans le but d'obtenir l'accès à une deuxième PC.	L'assertion peut contenir l'identité d'une PC à l'intention de laquelle l'assertion a été générée. Une PC vérifie si les assertions entrantes comprennent son identité en tant que récepteur de l'assertion.
	Réutilisation d'assertion – Un auteur de menaces tente de se servir d'une assertion qui a déjà été utilisée auprès de la PC visée.	L'assertion comprend une estampille temporelle et n'est valide que pour une courte période. Une PC vérifie l'estampille temporelle et la durée de vie pour s'assurer que l'assertion est encore valide. La valeur de durée de vie peut être inscrite dans l'assertion ou encore définie par une PC. Une PC exerce un suivi des assertions qui ont été employées pendant une certaine période (configurable) de façon à garantir qu'une assertion ne sera pas utilisée plus d'une fois pendant la période en question.
Authentifiants secondaires Les menaces de ce type ciblent les secrets temporaires qui sont transmis aux abonnés authentifiés et leur permettent de se faire reconnaître par une PC.	**Fabrication d'authentifiants secondaires** – Un auteur de menaces peut tenter de générer un authentifiant secondaire valide et de s'en servir pour se faire passer pour un abonné.	Un authentifiant secondaire peut comporter assez d'entropie pour qu'un auteur de menaces qui n'a pas d'accès direct au générateur de nombres aléatoires d'un vérificateur ne soit pas en mesure de deviner la valeur d'un authentifiant secondaire valide. Un authentifiant secondaire peut contenir des données d'assertion opportunes qui sont signées par un vérificateur ou protégées sur le plan de l'intégrité grâce à une clé partagée entre un vérificateur et une PC. Un abonné peut être directement authentifié auprès d'une PC grâce à son jeton à long terme. Ce faisant, il n'a plus besoin d'un authentifiant secondaire.
	Capture d'authentifiant secondaire – Un auteur de menaces peut recourir au détournement de session pour capturer l'authentifiant secondaire lorsqu'un vérificateur transmet celui-ci à un abonné après l'étape initiale d'authentification. Cet auteur de menaces peut tout aussi bien recourir à une tentative de MitM dans l'intention d'obtenir l'authentifiant secondaire lorsque celui-ci est utilisé	Pour qu'il soit protégé pendant sa transmission entre un vérificateur et un abonné, l'authentifiant secondaire doit être envoyé au moyen d'une session protégée initiée au moment de l'authentification initiale de l'abonné doté d'un jeton, semblablement au processus employé pour protéger les données sensibles contre les attaques par détournement de session. Pour éviter qu'il ne soit capturé pendant sa transmission à une PC, un authentifiant secondaire doit être utilisé dans un protocole d'authentification

Type de menace à l'assertion	Menace particulière	Stratégies d'atténuation
	par un abonné pour se faire authentifier auprès d'une PC. Si, comme dans le modèle indirect, une PC doit renvoyer l'authentifiant secondaire à un vérificateur dans le but d'en vérifier la validité ou d'obtenir les données de l'assertion correspondante, un auteur de menaces pourrait, de façon analogue, perturber le protocole de communication entre le vérificateur et la PC, puis tenter de capturer un authentifiant secondaire. Dans tous les scénarios présentés ci-dessus, un authentifiant secondaire peut être utilisé pour usurper l'identité d'un abonné.	qui assure une protection contre l'écoute clandestine et les attaques MitM. Pour qu'il soit protégé après avoir été utilisé, l'authentifiant secondaire ne devra jamais être transmis dans une session non protégée ni acheminé à une partie non authentifiée tant qu'il sera valide. Un authentifiant secondaire peut être envoyé en texte clair seulement si l'envoyeur a la garantie que l'authentifiant secondaire ne sera pas ultérieurement accepté par une autre PC. Ce cas de figure est possible lorsque l'authentifiant secondaire est particulier à une seule PC et que celle-ci n'acceptera pas d'authentifiants secondaires de même valeur jusqu'à ce que l'assertion correspondante ait atteint la limite de sa durée de vie.
Force de liaison du secret de l'assertion et de l'authentification Les menaces de ce type consistent en une manipulation des données d'assertion qui ne sont pas fortement liées aux secrets d'authentification.	**Substitution d'assertion** – Un abonné peut tenter de se faire passer pour un abonné privilégié (doté de droits d'accès plus importants) en s'en prenant au canal de communication entre le vérificateur et la PC, par exemple, en réordonnant les messages de façon à convaincre la PC que son authentifiant secondaire correspond aux données d'assertion envoyées au nom de l'abonné privilégié. Il s'agit là, principalement, d'une menace au modèle indirect, puisque dans le modèle direct, les données d'assertion sont directement codées dans l'authentifiant secondaire.	Qu'elles soient signées ou protégées sur le plan de l'intégrité par un vérificateur, les réponses aux demandes d'assertion peuvent contenir la valeur de la référence à l'assertion utilisée dans la demande ou quelque nonce qui aurait été cryptographiquement lié à la demande par une PC. Les réponses aux demandes d'assertion peuvent être liées à la demande correspondante selon l'ordre des messages, comme dans HTTP, pourvu que les assertions et les demandes soient protégées par un protocole, notamment TLS, qui sera apte à détecter et à rejeter les réorganisations malveillantes de paquets.

Annexe B Conseils sur la sécurisation des mots de passe

Cette annexe prodigue des conseils pratiques aux concepteurs de systèmes, aux opérateurs de systèmes et aux utilisateurs concernant la conception, la mise en œuvre et l'utilisation de systèmes d'authentification à mot de passe. Elle segmente également les exigences, mentionnées aux sections 4 et 5 du présent document, qui sont imposées aux parties responsables, et fournit des recommendations quant à leur mise en œuvre.

Cette annexe met l'accent sur les approches pratiques qui permettent de protéger les mots de passe contre les compromissions découlant des attaques en ligne ou hors ligne définies ci-dessous :

- **Attaque en ligne** – un auteur de menace tente de s'authentifier en tant qu'utilisateur légitime en essayant de deviner le mot de passe de l'utilisateur par essai-erreur. Une telle attaque peut être étroitement ciblée et éclairée par une quelconque connaissance de l'utilisateur ciblé, ou encore cibler un large groupe d'utilisateurs de manière opportuniste.
- **Attaque hors ligne** – un auteur de menace ayant obtenu accès à une base de données de condensés de mots de passe fait appel à des ressources informatiques spécialisées pour récupérer (ou craquer) les mots de passe.

B.1 Conseils aux concepteurs de systèmes

Les concepteurs de systèmes doivent concevoir des systèmes de TI qui permettent de faire peser le fardeau de la sécurité des mots de passe sur les systèmes plutôt que sur les utilisateurs. Ces conceptions doivent tenir compte des considérations énoncées ci-dessous.

B.1.1 Attaques en ligne

Les concepteurs de systèmes de TI peuvent limiter les riques associés aux attaques en ligne en mettant en place les mécanismes de sécurité suivants :

- **Surveillance** – La pratique exemplaire veut que tous les systèmes de TI assurent la surveillance des échecs de connexion. Pour accroître la résistance aux attaques en ligne, un système devrait mettre en correlation l'heure et la date de ces événements et les comptes des utilisateurs de manière à détecter les attaques ciblées lentes et de faible puissance communément appelées « Low and slow », ainsi que les attaques plus étendues visant l'ensemble des utilisateurs. On peut également avoir recours à une analyse plus poussée du comportement des utilisateurs pour détecter une utilisation potentiellement abusive des comptes compromis.
- **Verrouillage de comptes** – Pour mettre fin à une attaque, un système devrait être en mesure de verrouiller les comptes ciblés une fois que les limites fixées ont été atteintes. Un maximum de 10 tentatives consécutives ou de 100 échecs cumulatifs devrait être autorisé au cours d'une période de 30 jours.
- **Ralentissement artificiel du trafic** – Un système peut mettre en œuvre des mécanismes de ralentissement artificiel du trafic pour endiguer une attaque en ligne, notamment en introduisant un délai d'attente plus long après chaque tentative de connexion infructueuse.
- **Liste noire des mots de passe** – Une liste noire des mots de passe les plus communément utilisés peut être mise en place sur le système pour empêcher les utilisateurs de les utiliser. Lorsque des exigences

complexes sont imposées pour ce qui est de la composition des mots de passe, les utilisateurs tendent à sélectionner des mots de passe qui respectent des modèles connus (voir la figure 2). Si elle utilisée en conjonction avec d'autres mesures d'atténuation des attaques en ligne, une liste noire n'a pas à être exhaustive, puisqu'il sera déjà difficile pour l'attaquant de deviner les mots de passe.

B.1.2 Attaques hors ligne

Les concepteurs de systèmes de TI peuvent limiter les riques associés aux attaques hors ligne en mettant en place les mécanismes de sécurité suivants :

- **Hachage** – Les mots de passe ne doivent pas être enregistrés en texte clair. Il faut plutôt les rendre illisibles en faisant appel à une fonction de hachage cryptographique. Il conviendra d'utiliser une fonction de hachage conçue pour résister aux attaques hors ligne, comme la fonction de dérivation de clés fondée sur un mot de passe 2 (PBKDF2 pour *Password-Based Key Derivation Function 2*) et de procéder à au moins 10 000 itérations de l'algorithme de hachage.
- **Salage par mot de passe** – Avant d'être soumis au hachage, chacun des mots de passe doit être combiné à une valeur de salage d'au moins 256 bits générée aléatoirement pour chaque entrée. Ainsi, même si deux utilisateurs sélectionnent le même mot de passe, on pourra s'assurer de générer des condensés différents.
- **Keyed-Hash Message Authentication Code (HMAC)** – Pour renforcer la sécurité, on peut également utiliser une clé secrète générée aléatoirement comme entrée dans la fonction de hachage. Une telle clé doit être stockée dans un module de sécurité matérielle (MSM) pour en préserver la confidentialité.
- **Éviter les mécanismes laborieux** – Si les mécanismes de sécurité ci-dessus ont été mis en œuvre pour résister aux attaques en ligne et hors ligne, il n'est pas nécessaire de mettre en place d'autres mécanismes qui constituent un trop grand fardeau pour les utilisateurs (tel qu'il a été discuté à la section 4.3). Ces mécanismes peuvent inclure :
    - des règles de composition de mots de passe excessivement complexes;
    - l'expiration des mots de passe basée sur l'âge;
    - l'application de l'unicité par rapport à l'historique des mots de passe.

B.2 Conseils aux opérateurs de systèmes

Les opérateurs de systèmes devraient mettre en œuvre les procédures suivantes afin de prévenir et de détecter les attaques sur les mots de passe, et de prendre les mesures nécessaires pour intervenir advenant de telles attaques.

- **Prévention** – Les opérateurs de systèmes devraient mettre en place les fonctions de protection des mots de passe décrites précédemment dans la mesure où de telles fonctions sont offertes sur le système. Ils devraient également prendre connaissance des conseils des fournisseurs de systèmes applicables et adopter les pratiques exemplaires recommandées.
- **Détection** – Les opérateurs de systèmes devraient mettre en œuvre des mesures de surveillance pour détecter les attaques en ligne et hors ligne. Les échecs de connexion doivent être journalisés, puis mis en corrélation et examinés afin de détecter les attaques en ligne. Il conviendra également de surveiller l'utilisation fructueuse des justificatifs et de signaler toute utilisation inhabituelle aux fins d'enquête. En outre, il importe de surveiller l'accès à la base de données contenant les mots de passe et de détecter toute exfiltration depuis celle-ci.

- **Intervention** – Des plans d'intervention en cas d'incident devraient être élaborés de manière à faciliter la prise de mesures advenant des incidents liés aux mots de passe. Dans de telles circonstances, les mots de passe compromis lors d'une attaque en ligne devront être réinitialisés et toute utilisation potentiellement abusive des justificatifs devra faire l'objet d'une enquête. Advenant la compromission suspecte de la base de données contenant les mots de passe, il conviendra de réinitialiser dès que possible tous les mots de passe compromis.

B.3 Conseils aux utilisateurs

Les utilisateurs devraient comprendre le rôle que jouent la longueur, la prédictabilité et la réutilisation des mots de passe dans la protection de l'accès à leurs comptes. La longueur du mot de passe est importante puisqu'elle offre une protection contre les attaques en ligne et hors ligne. En ce qui concerne les attaques en ligne, comme la longueur des mots de passe est proportionnelle au nombre de valeurs composant les mots de passe qu'il est possible d'attribuer à un compte, un plus grand nombre de tentatives sont nécessaires pour les deviner. Quant aux attaques hors ligne, la mesure de sécurité la plus efficace que peut appliquer un utilisateur est d'accroître la longueur de son mot de passe.

S'il s'avère difficile de faire appel à des méthodes force brute, les outils de craquage déchiffront les mots de passe en faisant appel aux modèles conçus aux fins de recherche dans les bases de données contenant des centaines de millions de mots de passe craqués. En l'absence de règle de composition ou de liste noire des mots de passe, l'utilisateur n'aura comme seul recours face à ces outils de craquage que de se sensibiliser à ces modèles connus et d'employer un mot de passe imprévisible.

En outre, les utilisateurs tendent à « recycler » leurs mots de passe, car ils n'arrivent pas à mémoriser des douzaines de noms d'utilisateur et de mots de passe sur tous leurs systèmes de TI. Malheureusement, la protection du stockage des mots de passe est fonction du niveau de sécurité offert par le moins sécurisé de ces systèmes de TI.

En d'autres mots, les utilisateurs devraient sélectionner des mots de passe résistants aux attaques et veiller à en assurer la confidentialité. Pour résister aux attaques en ligne,ils devraient éviter d'utiliser des compositions courantes qui sont connues des attaquants, tel que l'illustre l'exemple à la figure 2. Les utilisateurs devraient également éviter d'inclure dans leurs mots de passe de l'information connue du public, comme leur nom ou leur ministère.

Figure 2 Mots de passes conformes, mais faciles à deviner

Pour résister aux attaques hors ligne, les utilisateurs devraient utiliser les mots de passe les plus longs et complexes que leur permet le système. Chaque caractère au-delà du minimum exigé par le système rend plus difficile le craquage du mot de passe.

Les utilisateurs ne doivent pas communiquer leurs mots de passe à autrui ou réutiliser les mêmes mots de passe pour leurs comptes professionnels.

B.4 Conseils sur l'utilisation des phrases de passe

Pour promouvoir l'utilisation de mots de passes plus longs, mais moins complexes, illustrée dans la présente, il conviendra d'envisager le recours aux phrases de passe. Une phrase de passe est un secret mémorisé qui se compose d'une séquence de mots ou d'un texte que le requérant utilise pour authentifier son identité. Bien que son utilisation soit similaire à celle du mot de passe, la phrase de passe est généralement plus longue, pour une sécurité accrue, moins complexe et plus facile à mémoriser pour les utilisateurs.

Toutes les exigences en matière de mot de passe définies dans la présente pour les jetons à secret mémorisé s'appliqueront dans la même mesure aux phrases de passe. En plus de ces exigences, il importe de tenir compte de ce qui suit :

- L'exigence en matière d'entropie ne sera pas moindre que celle exigée pour un mot de passe.
    - Si la phrase de passe est choisie dans une liste de mots prédéterminés, l'entropie, telle qu'elle est calculée en tant que fonction de la taille de la liste de mots et du nombre de mots, devra être équivalente ou supérieure à celle imposée aux mots de passe.
    - Si la phrase de passe est choisie par l'utilisateur, l'entropie, qui est calculée en tant que fonction des mots compris dans la langue choisie, des langues autorisées, de la longueur de la phrase et du nombre minimal de mots dans la phrase, devra être équivalente ou supérieure à l'entropie imposée aux mots de passe.
- On recommande que les systèmes d'entrée d'authentification prennent en charge un minimum de 64 caractères afin de permettre l'utilisation de phrases de passe.
- Plusieurs produits d'établissement de listes noires de mots de passe refuseront les mots de passe qui contiennent des mots figurant dans un dictionnaire. Cette restriction devra être désactivée afin de permettre l'utilisation de phrases de passe. Avec l'utilisation grandissante des phrases de passe, et l'extraction de listes de phrases de passe courantes depuis des ensembles de données sur les violations, les produits d'établissement de listes noires devront également être en mesure de prendre en charge des chaînes de phrases de passe.
- La plupart des produits d'établissement de listes noires peuvent vérifier la longueur des mots de passe, d'autres peuvent en vérifier la complexité, mais peu sont en mesure de procéder simultanément à ces deux vérifications. Sur les systèmes ne permettant pas la prise en charge de ces deux vérifications, il faudra dès lors incommoder soit le groupe d'utilisateurs de mots de passe, soit le groupe d'utilisateurs de phrases de passe.
- Des phrases de passe plus longues pourraient entraîner une hausse du nombre de tentatives infructueuses de connexion en raison des erreurs de saisie et on sait que les espaces sont aussi source de problème. Si le système le permet, les opérateurs de systèmes devraient envisager les mesures suivantes : filtrer les espaces ou regrouper les espaces répétitives (que ce soit lors de la sélection du mot de passe, ou en filtrant les données saisies par l'utilisateur en veillant à ce que le reste de la chaîne respecte la longueur minimale), modifier la longueur maximale des phrases de passe et passer en revue les valeurs de verrouillage basées sur les données opérationnelles.

- À l'instar des mots de passe, les maliciels (p. ex. les outils d'hameçonnage et les enregistreurs de frappe) ne portent pas attention à la longueur ou à la complexité des phrases de passe. Par conséquent, la protection de l'infrastructure d'authentification (détection d'anomalies de l'authentification, l'établissement de listes de noires, le salage et le hachage des mots de passe, etc.) est toute aussi importante que la mise en place de règles appropriées.